



# ***PX-P3000E100TP***

## ***Users' Manual 1.5f***

# Table of contents

<b>1</b>	<b><i>Introduction.....</i></b>	<b>4</b>
1.1	What is FSO?.....	4
1.2	Why is it important? .....	4
1.3	Optical Free-space Transmission .....	6
1.4	Typical applications .....	7
<b>2</b>	<b><i>Interfaces for the PX-P3000E100TP and technical specification .....</i></b>	<b>8</b>
2.1	100Mbps TP interface.....	8
<b>3</b>	<b><i>Sites of installation.....</i></b>	<b>9</b>
3.1	Key factors of operation .....	9
3.2	Preferred installation sites .....	9
3.3	Distance measurement.....	11
3.4	Direct sunshine .....	11
<b>4</b>	<b><i>Eye safety.....</i></b>	<b>12</b>
<b>5</b>	<b><i>The mounting bracket.....</i></b>	<b>13</b>
5.1	Fixing the heads.....	13
5.2	Alignment of the heads .....	13
5.2.1	Steps of the head fixation.....	13
5.3	Meanings of the LEDs .....	14
5.4	LCD screens.....	14
5.5	Inside the laserhead .....	15
<b>6</b>	<b><i>Alignment .....</i></b>	<b>15</b>
6.1	LCD panel (receiver) Alignment.....	15
6.2	Beam Alignment.....	17
6.3	Set the beam size .....	18
<b>7</b>	<b><i>System installation .....</i></b>	<b>19</b>
7.1	On the table test .....	19
7.1.1	Alignment of the <b>PX3000E100TP</b> .....	20
7.1.2	Connecting to your Network.....	21
<b>8</b>	<b><i>Management.....</i></b>	<b>22</b>
8.1	Features.....	22
	Login Screen and password .....	22
	Head information screen .....	22
	Status info screen .....	23
	Device setup.....	24
	IP Setup.....	25
	SNMP Setup .....	26

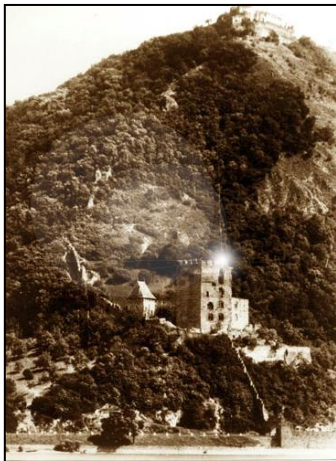
Security .....	27
Network statistics page .....	27
PX-P3000E100TP0 extra MGM features .....	29
Mandatory Management Activation .....	30
<b>8.2 Firmware update.....</b>	<b>31</b>
<b>8.3 Reloading factory default settings .....</b>	<b>33</b>
<b>8.4 Setting up the SNMP .....</b>	<b>33</b>
8.4.1 SNMPc Installation.....	34
8.4.2 Configuration of the SNMPc Management console .....	35
8.4.3 Compiling GeoDesy-FSO Mib file.....	38
8.4.4 Using SNMP to monitor the link .....	40
8.4.5 Generating failure .....	42
8.4.6 SNMP Technology.....	44
Trap event list .....	51
<b>9 Warranty conditions.....</b>	<b>52</b>
<b>10 Privacy statement .....</b>	<b>53</b>

## 1 Introduction

### 1.1 What is FSO?

**FSO** is free space optics provides point-point broadband communications using Laser Light as the transmission medium.

**FSO** is a state of art data communication method which is based on a very old communication solution. Ancient Chinese developed a protection system against the Mongol tribes, building watchtowers within the line of site to other towers. And as soon as the towers saw some hostile sign on the horizon they use they shield to reflect the sun to the remote towers. In this way the area could be prepared against the attack in a very short period of time.



In the ancient times for this communication use the mirror as a transmitter and the sunlight was the light source, and the receiver was the remote guard's eye. This basic signalling method was developed later into up communication device which used „line coding”. This allowed the guards to tell the number of enemy, or the direction they are coming from.

Current **FSO** systems use a laser-diode as a light source, and a receptor diode (photo diode) to receive the signals coming from the laser diode from the transmitter side. But the basic elements are still the same: line of site between the communication nodes, and individual line coding. It is all about performance. **GeoDesy FSO** offers **FSO** systems with the highest power budget available on the market.

### 1.2 Why is it important?

Because of in the ancient Chinese times, the rain, the fog, or even the cloudy weather, could impact the operation of the whole system.

In the **FSO** units, comprising light source and receiver the cloud problem was solved, but development conditions still can impair performance. To go throw the rain, the fog, or snow you need more and more power to be seen from the remote side. Achievable power levels are limited by a number of factors including eye safety.

In this way there is no other choice to see more than „training the eye”. Making the receiver more and more sensitive to sense delight emitted from the remote side.

**GeoDesy FSO** offers high transmit power and also very hard receiver sensitivity. These two factors combined to provide one of the best performing **FSO** systems on the market today.



To meet the demands for every higher bandwidth, **GeoDesy FSO (Europe) Limited** continues to invest heavily in research and development with the newest product line which offers Gigabit speeds being launched.

This manual describes the **GeoDesy FSO Next** series of free space laser transmission system.

The **GeoDesy FSO Next** product range offers cost effective reliable free space laser transmission for two Mbps up to 1000 Mbps data to the air, where a clean line of site is available. It delivers the most effective point-to-point connection between computer networks or telephone exchanges.

No need for installing cables, no rental costs, no licensing requirements.

Ideal for urban areas or city centres, where the use of these lines are expensive. Suitable for factories or industrial environments where high noise level can interfere with the transmitted data. The best choice to make a connection across rivers and other natural or artificial obstacles, where cable is not available.

The transmission technique used in the **GeoDesy FSO** devices provides transparent and wire-speed data transfer with virtually zero latency. Because they use infrared light as the transmission medium, **GeoDesy FSO** system do not require frequency licenses and the transmission is not effected by electro-magnetic or radio-frequency interference. Basically the **GeoDesy FSO** link can be considered as a virtual fibre in the air, which ends in real fibre optic cable at both ends.

Our product is built using high quality components for operation in even the most adverse conditions.

Metal housing gives robust, waterproof environment for the electronics.

The shield protects the device from direct sunlight and provides extra air isolation.

The **GeoDesy FSO X** systems comprise two laser-heads and the two indoor interconnection units (OIU) - one at each end. The interface connections are housed in the outdoor unit together with the PSU of the system.

Best practises were employed in cost engineering throughout the development of **GeoDesy FSO**.

## 1.3 Optical Free-space Transmission

The principle used in free space laser transmission is very similar to the one is used for fibre optic transmission. The difference is while fibre optic devices use electronics and optics optimized for transmission to the air. Also one can observe to the similarity in the transmission properties. No galvanic contact, no ground-loops, no need for surge protection, noise immunity, long distances, high bandwidth.

What makes it unique – and difficult to design – is that it does not require any transmission medium like fibre or copper, but it has to cope with the dynamically changing parameters. For instance while the attenuation of an optical fibre is constant, the attenuation of the atmosphere between the laser units can change dramatically (depending on the weather conditions).

The laser-heads are usually placed on top of building, where the clean line of site is guaranteed and the beam cannot be interrupted.

In the head the incoming signal is amplified, encoded, and then drives the laser-diode. The transmitter optics assures the proper beam shape and controls the beam divergence. The receive optics perceives and directs the transmitter signal to the photo diode. The diode converts it back into electrical, than it is decoded, amplified and converted.

There are several things that can influence the quality of transmission. We can classify those factors into three main groups.

System conditions - transmitting power, transmitter's wavelength, beam divergence, receiver optics diameter, receiver sensitivity, parameters of optical system and casing. These parameters determine the system's characteristic at a certain distance and are controlled by system design and factory set up.

Weather conditions - molecular absorption, particle scattering and turbulence. These elements have great effect on the operational conditions of the system. We do not have very much influence on them; proper product selection can eliminate the undesirable effects.

Environmental conditions - building movements, direct sunlight, refractive surfaces. These are also key factors related to the installation sites and can be controlled by appropriate site survey and system installation

## 1.4 Typical applications

Most typically the **GeoDesy FSO Next** products are used to interconnect LAN-s. The system is protocol transparent, thus other applications also can be taken into consideration. Appropriate interface converters are needed and system bandwidth must be matched for that.

Here we collected some circumstances, where the deployment of the **GeoDesy FSO** is the most adequate as a cost effective solution.

Those are:

### ***Areas with natural or artificial obstacles***



Where cable is actually not an alternative, like across rivers or railways or in rugged terrain.

### ***Urban areas***

Where only leased lines are available with limited speed, and high rental cost. With GeoDesy FSO links you can establish on line LAN-to-LAN connections.



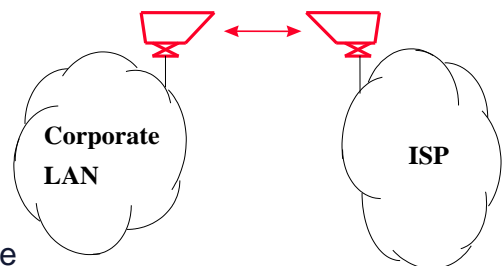
### ***Industrial areas***



Where you have noisy environment with high EMI or RFI. Factory buildings, airport objects can be connected through laser link.

### ***ISP connections***

Where high bandwidth is required. ISP's can offer high-speed links to their customers or trunks can be established between ISP's instead of expensive leased lines.





## 2 Interfaces for the PX-P3000E100TP and technical specification

### 2.1 100Mbps TP interface

The **GeoDesy FSO X PoE** series products are designed to provide easy-to-use and cost-effective solution for interconnecting Local Area Networks. By utilizing standard Category 5 cable and using standard IEEE802.3af interface the deployment of the system is easier than ever before. The transparent and wire speed data transfer together with virtually zero latency assures the easy integration of the system in all environments.

The **X PoE** systems should be considered as repeaters in the network. So the installation distance between the head and the network device is 100m. The distance on a back to back site is maximum 5 meters, between the heads without signal regeneration.

The **X PoE** systems connecting to the network with an RJ 45 cable which provides the power required for operation and the data. The system requires IEEE 802.3af Power over Ethernet switch or power injector. The power consumption suits to the standards described in the standard. Also provides fast and easy connection for the management system for more details please see the chapters below. The system is certified **Class 1M product**, this way 100% eye safe.



## 3 Sites of installation

### 3.1 Key factors of operation

There are four key issues that the site survey has to shed light on. Proper system operation cannot be guaranteed without satisfying all of the four requirements.

**Clear line of sight** - The entire optical path between the two ends must be free of any obstacles. It not only means that one has to see the other side, but other possible sources of disturbance should also be taken into consideration. For example there might be turbulence above the roofs and other constructions, and this can cause fraction or scattering of the beam or snow accumulation on roofs too close to the beam can influence or even interrupt communication.

**Solid mount surface** - is the key for long-term operation. Since the diameter of the beam is limited, it is extremely important to mount the unit on a stable structure with the possible smallest movement. This way the receiver of the remote unit cannot get out of the beam due to the movement of the opposite head.

**East-West orientation** - although the receiver optics are equipped with optical filters to protect the receiver diode from the effect of undesired light sources, direct sunshine can cause saturation of the diode. This prevents the system from working properly for several minutes a day at certain times of the year. In most cases this effect can be avoided by careful selection of the mounting spot.

In order to comply with the requirements of the successful installation - including the discussed four key factors and other criteria - the following matters should be taken into consideration.

### 3.2 Preferred installation sites

All buildings and constructions have a certain movement of their own. It's determined by the structure and material of the building. Metal structures can shift or twist due to temperature changes. Wooden construction can expand or shrink with any changes in humidity. Give preference to concrete or brick buildings. On the other hand high structures like towers, skyscrapers or poles are always subject to movement. Mount the support frame to walls of the building or near corners, as they are the most stable spots. Use appropriate consoles for wall mounting. If a stand is used on the top of

building, secure it directly to the ceiling or to the concrete cornice wherever is possible. Do not fix stands to insulating materials as they can slowly sink under the weight of the unit and with temperature changes. Big chimneys and smokestacks may look stable, but as their inner temperature varies they can also move. Vibration caused by heavy traffic, trains and elevators etc. may slowly move the system out of its specified direction. Another important consideration is to provide enough space for alignment and to have the potential for future maintenance. Consider that the support frame is usually heavy, so the selected spot should be easily accessible.

<b><i>Preferred installation sites</i></b>	<b><i>Pay attention to</i></b>	<b><i>Avoid (*)</i></b>
Concrete wall	Behind window	Soft materials
Brick wall	Old constructs	Chimneys
	Microwave towers	Wooden constructs
		Metal masts or Frames
		Hidden heat isolations, like Styrofoam

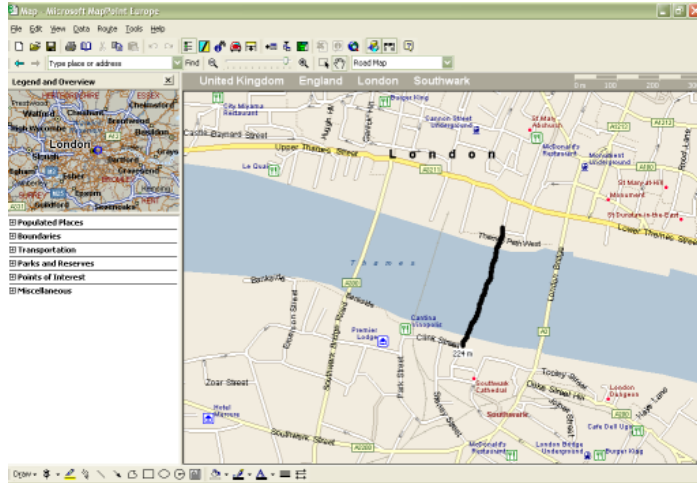
(\*)

*In cases where installations are listed under "AVOID" cannot be avoided than special mounting accessories to be designed and special installations must be used.*

It is not only the building that has to be solid, but the support structure too. Antenna poles and security camera holders are not suitable for the **GeoDesy FSO** units.

### 3.3 Distance measurement

Because the units were designed, and calibrated for certain distance operations the higher distance will decrease the availability. GeoDesy FSO pre-calibrates and pre-tests every unit shipped to the customer. To ensure that the unit you are about to



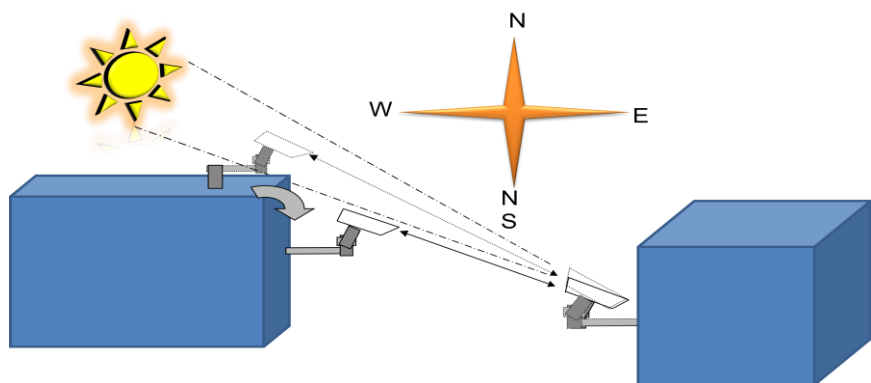
buy fits to the needs, the first step is to measure the distance. The best way to measure it is by GPS (Global Positioning System), these units are accurate enough to determine the distance between two points. For more details please refer to the GPS manufacturer handbook. Also there are several other ways to measure the distance. If you know the exact



address you can use mapping software like MapPoint or Auto route.

### 3.4 Direct sunshine

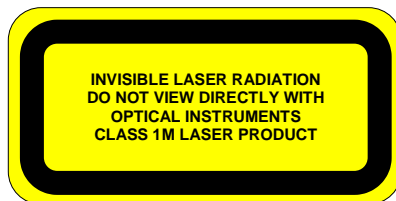
To prevent the sun shining directly into the receiver optics, first one has to determine the orientation of the link. Try to avoid East-West orientation wherever it is possible. Examine both sides of the link at sunset and sunrise and find a position where the sun cannot get behind any of the heads. Be aware that the path of the sun is changing throughout the year.





## 4 Eye safety

There are no two installation spots of the same kind, the buildings or structures, the available space and the accessibility of the place will be different in each case. Nevertheless, as a general rule it is very important to select the installation site so that nobody can look directly into the transmitter. For this reason place the head either so high (on the side wall of the building) or so close to the edge of the building (on a parapet on the rooftop) that no person can approach it accidentally and can get into the beam path. Set up barriers if necessary and put warning signs at prominent places.

The laser heads are provided with all labels and hazard warnings required by the laser standard. There are warning labels on both the left and right side of the protective cover next to the optical window and there is a warning and an informative label on the rear side of the laser head.



 	
Type	: LB PX-P3000E100TP
S/N	: LBH-«s/n»
Input Power	: -48VDC IEEE 802.3af compliant
Laser	: 1M
Wavelength	: 860nm
Manufactured by: GeoDesy FSO 1162 Budapest, Kondorfa u. 6-8, HUNGARY, Tel.:+36-1-453-7440 Fax.:+36-1-240-3570 <a href="http://www.GeoDesyFSO.com">www.GeoDesyFSO.com</a>	

## 5 The mounting bracket

### 5.1 Fixing the heads



Your PX-3500E100TP head can be fixed to its stand with an Alignment Base Unit (ABU). On the figure you can see an ABU, and a plinth of a PX-3000E100TP unit, and the necessary fixing parts. The necessary nuts and washers can be found on the legs of the head. The steps of the fixing are.

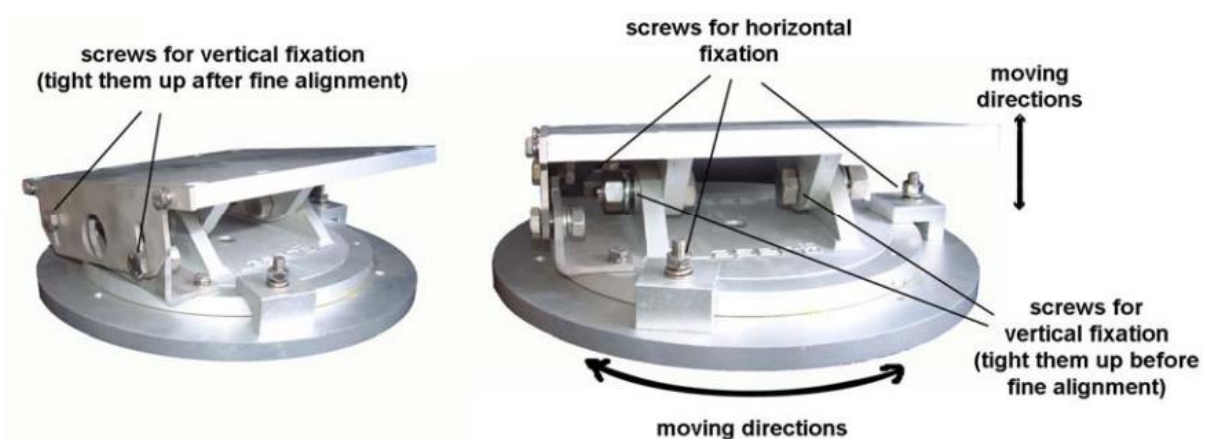
- First, fix the Abu to the stand using the washers and nuts
- Place the head to the ABU
- Fix the bolts with the nuts, using the washers
- Tight up all the nuts

### 5.2 Alignment of the heads

#### 5.2.1 Steps of the head fixation

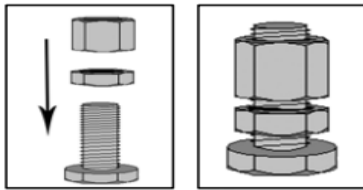


- Target Side B with the crosshair built in to the head on Side A!
- Screw the two nuts up tight on both heads, which are used for the fixing the vertical direction, but be careful that the heads do not move out from its position!
- Screw the three nuts up tight on both heads, which are used for the horizontal fixation, but be careful that the heads do not move out from its position!
- Repeat this on the other side of the link!

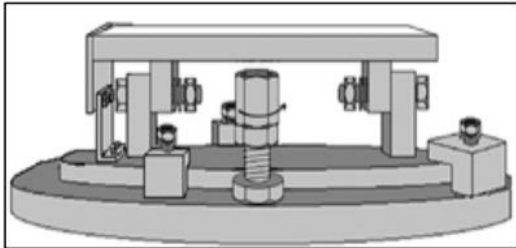


- Place up the spacers on both sides!

Place the two spacers where the figure shows to.



Open the spacers until it reaches the bottom of the upper plate of the ABU! Repeat this on the back side too!



Then do the same on the remote side too!

## 5.3 Meanings of the LEDs

**Power:** The head is powered up.

**RX-OK:** Received beam is good for communication.

**TP Lk:** Copper link between the head and the Network equipment.

**FO Lk:** The received signal from the remote end is modulated and .

**R-V/TP:** Remote end is visible for the management system and there is TP connected to remote end – same as TP-Lk but displays it on the remote end.



## 5.4 LCD screens

Please press the button on the backside of the unit to scroll between the screens!

### 1.screen

Loc (local level): Light received from the remote end.

Rem (remote level): Remote Sites Received level.

Op: optimal

Ov: overload



### 2.screen

HeadSN: The laser head serial number  
0000001



### 3.screen

Temperature: Temperature inside the laser head.

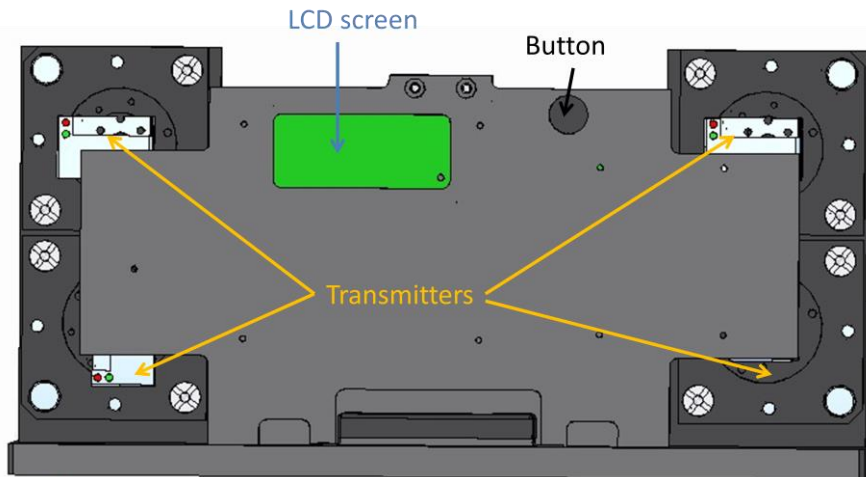
TT°C

### 4.screen

[tech@geodesy.hu](mailto:tech@geodesy.hu)

## 5.5 Inside the laserhead

**Warning** only trained personal should open the casing. No user servicable part inside.



## 6 Alignment

The very first step is to power up the heads. After this the boot sequence should run down, which takes 10-15 seconds.

### 6.1 LCD panel (receiver) Alignment

**Important!** For alignment purposes you might need a computer connected to the system. The adjustment of the motor control, and the switching of the transmitters are possible with a PC.

For adjustment please see PX-3000E100TP extra MGM functions chapter.(30 page)  
For manual disabling please follow the below:

- Turning off the motor control: Restart the laser head during boot and pull out the plug while booting. After plugging in the motor controller will turn off.

The motor control is a “light-buffer” this saves the power for the bad weather and in the same time protects the receiver against overload.

During the alignment it can be used manually, to avoid the saturation, and keep the detector voltage on the level where it can be still monitored. The detector voltage can be increased to seven volts; above seven volts you won't be able to monitor the detector voltage.

This plate is located in front of the receiver, and you can rotate it (clockwise decreases the detector voltage, counter- clockwise increases).



- Follow the steps below
  1. Switch on one of your transmitter on one side, and switch off all the others.

Switch off the transmitters on the other side too. You can adjust the transmitters only in the management. Please take a look at the PX-3000E100TP extra MGM features chapter.(30 page)

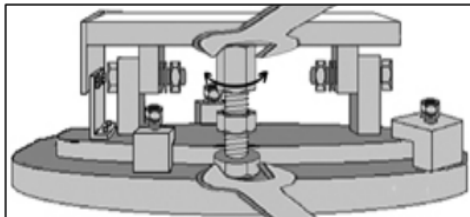
You can check which transmitter is in use, in the management (refer to page 30) with the Local level LEDs of LCD on the back of every transmitter.

Each LED indicates the transmitters are functioning, and transmitting.

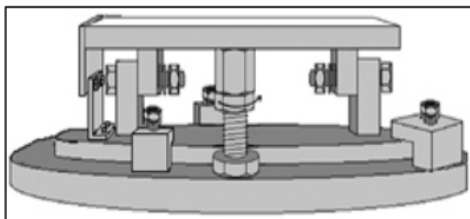
2. Move the head with the off switched transmitters until you can get the biggest incoming light efficiency on the other side.
3. Fix the head as hardly as you can!
4. Repeat this with the other head too.

The receiver alignment should be done on both sides; the requirement is some incoming light from the remote side (at least receive). This alignment will determine the position of the head and in the position of the receiver. The idea is similar to the focusing, but the only way to find focus is to move the head. You can check the incoming light efficiency in two ways. You can use the level on the LCD screen.

**On the LCD screen you can see the remote level of the other Laser Head!**



Because of the weight of the heads for the vertical moving you can use the spacers as it is shown on the figure. For this moving you need two wrenches. With one of them you have to hold the head of the bolt, and with the other you can turn the thick nuts to lift or loose the plate of the ABU!

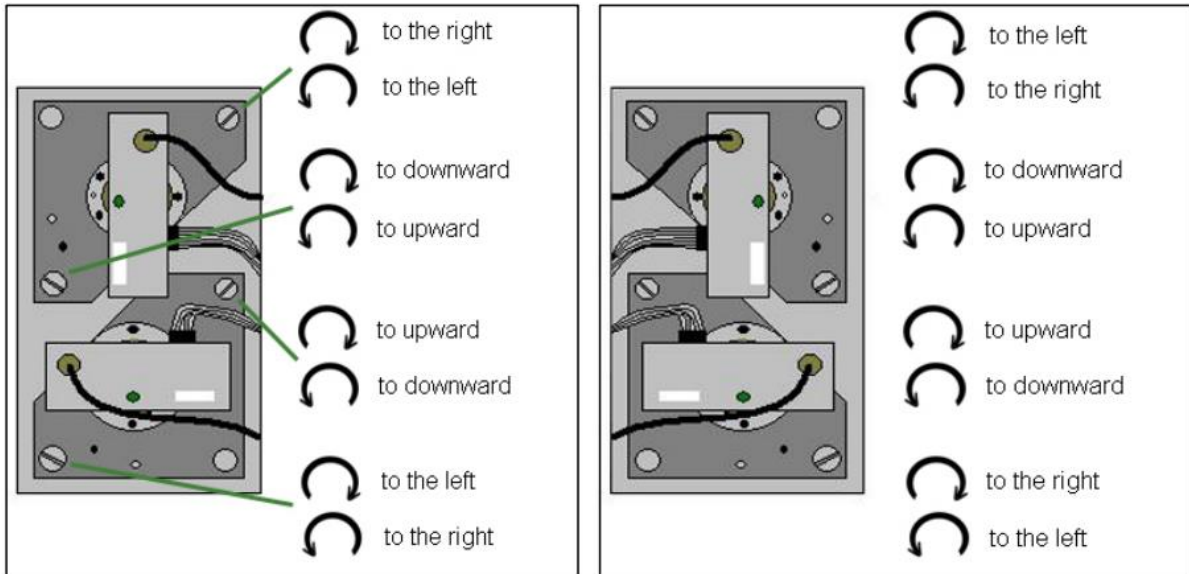


To not enable any movement after the receiver alignment on the vertical angle of the head and due to the heat expansion please close the locking nut under the thick nut, as it shown on the figure, on both sides.

Please not before the vertical receiver alignment we strongly suggest doing the horizontal the same way as it is written above.

## 6.2 Beam Alignment

- Switch off all of the transmitters on both sides.
- Switch on one of your transmitters on one side.
- Move the beam the middle of the remote head.

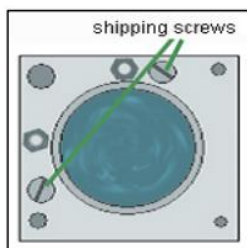


You can move the beam with the screws on the back of the transmitters. The directions of beam moving in the function of the turning direction of the screws can be seen on the figure.

You can check the position of the beam using a digital camera with infrared lenses. You can see the beam shining on the landmarks around the remote head from the side of the transmitter, or until dusk you can see the line of the beam with your own eyes.

From the remote side you can see the light of the beam behind the head with the shadow of the head on a surface (for example on a wall), or if you see toward the side of the transmitter, there you can see shining the beam on landmarks, and with the growing and declining of the shining rounded plate, which is the beam, you can follow its moving.

- Repeat the beam alignment with each transmitters on both sides.

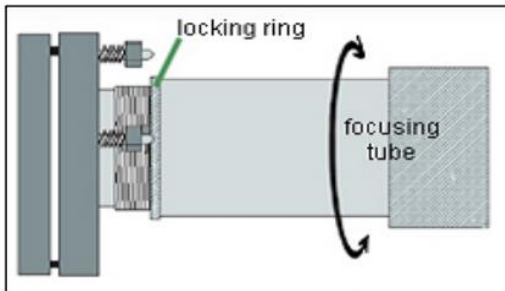


In every transmitter there are two shipping screws against the bigger moving of the tube. These screws allow only less movings for the transmitters, so if you need bigger moving you have to pick them out first.

Anyway, GeoDesy-FSO strongly recommends that you take all of them out first...

### 6.3 Set the beam size

You can set the beam sizes of each transmitter separately. So do not switch on more than one transmitter in the same time!



You can set the beam size turning the focusing tube. First you have to loose the shipping screws which are functioning as transmitter fasteners, during shipment. Then you have to loose the locking ring which fastens the focusing tube. After that you can manipulate with the beam size turning the tube. If you turn it in clockwise direction the

diameter of the beam will increase, and in counter-clockwise direction the beam size will decrease.

After you set the beam size, do not forget to lock the locking ring and tight up the two shipping screws, but be careful that the transmitter does not move out its position!

The provide the excellent operation you need the following beam sizes:

On 3000m distances the diameter of the beam should be 3meters!

On 3250m distances the diameter of the beam should be 3,25 meters!

On 3500m distances the diameter of the beam should be 3,50 meters!

On 3750m distances the diameter of the beam should be 3,75 meters!

On 4000m distances the diameter of the beam should be 4 meters!

You can measure your beam size using a digital camera with infraed lenses. With this you can see the beam behind the head on a surface (for example on a wall) and there you can measure it. In that case if there are not any surfaces for beam measuring, you can do it in the following method:

Face the remote side and check the beam with your camera. Move slowly to the right in straight line until the picture of the beam, what you see in the camera, is reducing, and sign that place. Do the same on the left side. Then you can measure the distance between the twosigned places. That will be the diameter of the beam. If you can not use the camera efficiently enough, you can do it with your own eyes too. The method is the same with one difference, the border of the beam is where. You cannot see the red dot on the transmitter lens of remote side.

Repeat the setting on both sides with all of the transmitters!

End of the alignment

- Switch on all of the transmitters!(in MGM)
- Reboot the laser head.
- Close up the covers of the heads!

## 7 System installation

### 7.1 On the table test

**Warning!** Do not look either into the transmitter or the receiver optics because at this distance even the reflected laser beam *can* be dangerous to your eyes. Operating the system on much shorter distance than presumed originally can cause saturation or even permanent damage to the receiver. Always use optical attenuators for this kind of test.

The on-the-table test needs careful planning and careful use during the test period. The units should be placed at about 2 m distance from each other with optical windows facing one another. Put an appropriate optical attenuator (Attenuating foil or cardboard with several small holes) between the heads. Make all the necessary connection as described below to connect your network equipment (computer or protocol analyzer) to the heads and power up the units. Turn ON the Outdoor Interconnection Units and check if the power LED is ON on the head.

You should be able to align the units without any tool and get full received level on the signal strength LED's. Make sure that the "Saturation" indicator is OFF. Adjust your attenuators if necessary to avoid saturation of the receivers.

Please note that at this short distance, specially the longer distance links can reflect to the remote site or even to the same head. If you experience full receiving level, with no traffic throughput, in that case try to move the heads slightly units out of the reflection zone.



Please also take in consideration that the laser beam is concentrated and in such a short distance can harm your eyes, every time you test the units on short distance, do it with extra care. Never look into the sighting device if the remote laser is turned on. We strongly suggest to double check the power connection before you turn on the device. Handle the power connection with extra care. Safety first.

After obtaining the desired received level, check the data connection between devices. Using computers or appropriate testing devices.

On the table tests are perfect for troubleshooting (If there is a transmission problem, check the status of the connecting devices (e.g. Link signal or cable polarity) and cables.) in a controlled area. If you experience some problems during the test, please try to test the connected equipments with a direct connection.

The first step after the unit was placed to the bracket, and the units facing each other.



Power      RX OK      TP-LK      FO-LK      R-V/TP



The diagram illustrates the PX-P3500E100TP system architecture, showing two sides (Side A and Side B) connected by a central blue arrow labeled "PX-P3500E100TP". Above the arrow, a red double-headed arrow indicates a range of "3100m-6000m".

**Side A (Left):**

- A **GeoDesy 150** device is connected to a **POE Injector** via a **TP cable for data**.
- The **POE Injector** is connected to an **Ethernet switch** via a **DATA** cable.
- The **Ethernet switch** is connected to two green server racks and two desktop computers via **DATA** cables.
- The **POE Injector** is also connected to **Main Power** via a **Power over Ethernet Power&Data** cable.

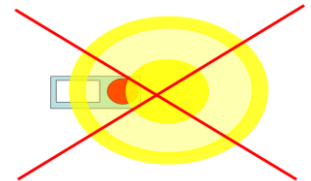
**Side B (Right):**

- A **GeoDesy 150** device is connected to a **POE Injector** via a **TP cable for data**.
- The **POE Injector** is connected to an **Ethernet switch** via a **DATA** cable.
- The **Ethernet switch** is connected to two green server racks and two desktop computers via **DATA** cables.
- The **POE Injector** is also connected to **Main Power** via a **Power over ethernet Power&Data** cable.

### Trick for the reliable alignment

A diagram of a cell. The cell is represented by a large yellow oval. Inside the cell is a smaller yellow oval representing the nucleus. To the right of the nucleus is a red circle representing a mitochondrion. The red circle is partially enclosed by a green rectangular outline, which represents the cell membrane.

set to this ring but this is far not as big as the core part of the beam. So every time you have an alignment please make sure that when you see the maximum LED s or a relatively high received level. Keep on moving to determine where the core part of the beam is. This can be done easily by looking at the received level you will see that the received level moves up then it will start move down than up again. During this time you just had the head moving into one direction. If you have any doubt on how to do the alignment please contact your distributor for further



20

## 7.1.2 Connecting to your Network

PoE 802.3 af connection.



PoE system is connected to the network via one twisted pair cable. This provides the power and the data for the GeoDesy FSO PX-P3000E100TP laser head .

The unit has connection for the management on the bottom of the Laser unit.

Please see the connection below.

This is the standard IEEE802.3af connector layout.

1. Orange/White	TX+
2. Orange	TX
3. Green/White	RX+
4. Blue	+VIN
5. Blue/White	+VIN
6. Green	RX-
7. Brown/White	-VIN
8. Brown	-VIN



## 8 Management

### 8.1 Features

The **Inband** network-monitoring unit is a newly developed highly featured monitoring for GeoDesy FSO manufactured laser links. This high quality equipment allows the user to monitor the link statuses such as detector voltage transmitter status, and many other features of the Laser link. Nevertheless, this chapter is intended to describe the usage of this network monitoring, and its connection and relationship with the GeoDesy FSO laserheads.

The Monitoring system is a standard feature in the PX-P3000E100TP system. For PX-P3000E100TP it is an optional and has to be activated. After the activation was purchased, with the invoice number, and the device serial number contact GeoDesy FSO technical support, for activation code. For further information check Activation chapter.

**Inband** monitoring is providing information about

#### Login Screen and password

The GeoDesy FSO unit arrives with preset values. Such as user name and password. We strongly recommend you to change the password after the unit was installed. The default username is admin, and the password is admin. If you forget your password contact technical support to receive your fail-safe password.

#### Head information screen

The head information screen is the main navigation panel through this screen you will be able to navigate into the submenu, of the monitoring system.

*Device Name:* displays the name of the device. Individually can be changed

*System Uptime:* Displays the lapsed time from the last boot of the device

*IP address:* Displays the IP(Internet Protocol) address of the device which must be a unique identifier in the network.

*Managed head:* displays the managed head type.

*Head Serial Number:* This is the head serial number and during the Activation process we will ask for this number.



## Status info screen

Clicking on the Device Setup you will enter the main status information screen, which will give you good summarized information of the device, such as status information of the transmitters, detector level, or temperature values.

Head status			
<b>Transmitter(s) signals:</b>			
Laser ON:	ok		
Laser OK:	ok		
<b>Analog values:</b>			
Temperature:	ok	26 °C	
Detector level:	error	0.06 V	
Remote Detector level:		0.00 V	
<b>Interface status:</b>			
TP_Link:		100M, Full	
FSO_Link:		No Link	
Remote is visible:		error	
Remote TP Link:		NA	
<b>Power supply:</b>			
PSU:		ok	
<b>Receiver status:</b>			
Rx OK:		error	

[Back to Prev page](#)

**Laser ON:** Transmitter transmits

**Laser OK:** Transmitter works properly, transmits and the transmitted signal is valid.

**Temperature:** ambient temperature inside the device. These units were designed for extreme conditions and should not have any problems under -60C to +80C. In fact the unit is emitting some heat so the temperature displayed is not the air temperature outside the head. For example the temperature can be -10C outside but in the device it won't go below -1 or -2. The value will display error depending on the setting was done device setup. There is no default value for this setting, only a suggested value, which is 60C.

**Detector level:** shows the local heads received level. In volts, the maximum is 7 volts and the minimum is 0.2 volts. The value will display error depending on the setting was done device setup.

**Remote Detector level:** this value is displayed from reception of the remote head. The maximum is 7 volts and the minimum is 0.2 volts.

**TP\_Link:** displays that there is connection over the TP cable.

**FSO Link:** displays that there is valid signal received from the remote end.

**Remote is visible:** this status information is a good information about the connection over the two laserheads if this status is OK that means that there is data transferred over the link.

**Remote TP Link:** shows that whether the remote end is connected into the switch and the TP interface is available.

**PSU:** The PSU of the device is sending the OK signal.

**RX OK:** this information is showing that the receiver is enabled. It basically means that there is valid signal with necessary strength is received in the local end.

## Device setup

The device setup screen leads you to the main monitoring options. Here the alarms can be set and main information about the Laser head.

BitView Web	
Managed device settings	
Device name: <b>LB-WEB</b>	<a href="#">Change</a>
Managed head: <b>2 - Pinto-X</b>	
Detector alert level: <b>0.50</b>	<a href="#">Change</a>
Temperature alert level: <b>70</b>	<a href="#">Change</a>
Auto MDI/MDI-X: <b>enabled</b>	<a href="#">Change</a>
Motherboard Firmware version: <b>3.0.1134</b> File image version: <b>071A</b> Motherboard Serial number: <b>000001</b> Head Serial number: <b>000001</b>	

[Back to Prev page](#)

Device name: unique identifier of the device

Managed head: Type of the laserhead

Detector alert level: when the received level reach this value, the alarm will be triggered.

Temperature alert level: when the temperature reach this value, the alarm will be triggered.

Auto MDI/MDI-X: this enables the Auto setting for the MDI/MDI-X, some old switch types might report incompatibility here it can be switched off. (Auto MDI/MDI-X can be turned off even in the Xs systems)

Motherboard Firmware version: This is the version number of the Firmware

File image version: Version number of the file image

Motherboard Serial number: Mainboard serial number inside the head (Not the same as the Head Serial Number)

Head Serial number: Serial number of the unit. Should be the same number as the one on the back of the unit. If the number is missing or not match up with the one on the back, during activation this is the number you will have to let the support know.

## IP Setup

Clicking on the IP Setup link you can have access to the Ethernet module of the system, this will make easy access to the IP number and/or port settings. These settings are sensitive setting and some of them cannot be restored by the user. Please always do the changes with extra care! If you have doubt in any step, do not hesitate to contact the technical support of the manufacturer website for further information.

IP information	
IP address: <b>192.168.100.221</b>	<a href="#">Change</a>
Subnet mask: <b>255.255.255.0</b>	<a href="#">Change</a>
Default gateway: <b>192.168.100.1</b>	<a href="#">Change</a>
Mac address: <b>00-50-C2-19-30-05</b>	
Remote IP address: <b>192.168.100.220</b>	<a href="#">Change</a>

[Back to Prev page](#)

**Local IP:** the IP address of the local device can be set in this box. If the IP address is set retype it to your browser.

Enter only valid IP addresses, if you forget the IP address, you will have to turn to our support and in some cases return the device for resetting the IP address. Please always do the IP change with care.

**Subnet mask:** you can set the subnet mask of the local device.

**Default gateway:** The default gateway setting for the local device.

**Remote IP:** This will tell this device what the IP address of the remote device is.

This setting wont change the remote units IP address, this just identify the remote device for the local device. If the IP address is not valid all diplays will go error and the display of the remote sites received level on the laserhead will be disabled!

192.168.100.220
set value: <input type="text"/>
<a href="#">Set</a>
<a href="#">Close</a>

255.255.255.0
set value: <input type="text"/>
<a href="#">Set</a>
<a href="#">Close</a>

192.168.100.1
set value: <input type="text"/>
<a href="#">Set</a>
<a href="#">Close</a>

192.168.100.220
set value: <input type="text"/>
<a href="#">Set</a>
<a href="#">Close</a>

## SNMP Setup

One of the main features of the device is the SNMP(Simple Network Monitoring Protocol). The SNMP settings can be set on this page.

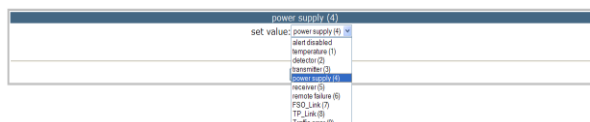
Snm information		
Trap address:	0. 0. 0. 0	<a href="#">Change</a>
1. trap event:	power supply (4)	<a href="#">Change</a>
2. trap event:	alert disabled	<a href="#">Change</a>
3. trap event:	alert disabled	<a href="#">Change</a>
Read community:	public	<a href="#">Change</a>
Read-write community:	public	<a href="#">Change</a>
Agent UDP Port:	161	<a href="#">Change</a>
Trap UDP Port:	162	<a href="#">Change</a>

[Back to Prev page](#)

Trap address: The IP address of the SNMP trap over the network.

Trap events in the system you have possibility to setup three different trap event.

For further details on the trap event see Trap event list chapter of this book. In this section there are the settings of the SNMP Agent.



SNMP trap address: IP address of the SNMP tarp computer

Read Community and Read Write community To the setup of the Read and the Read-Write community, the preset value is public

Agent UDP Port the SNMP agent UDP port number (1...1000) the preset value is 162

Trap UDP Port: the SNMP trap UDP port number (1...1000) the preset value is 161

Traps:

The Laserhead is sending two different traps:

**LaserHeadAlarm** (OID: 1.3.6.1.4.1.17857.0.1201) This trap will be sent after any of the alarms will go on (for alarm setting please see chapter 5.4)

**LaserHeadAlarmCancel** (OID: 1.3.6.1.4.1.17857.0.1202) After the alarm goes off this trap will be sent

## Security

On the security section you can set the username and the password for the unit. If you have forget the usernam and/or the password please contact The technical support.

Security information		
Username:	<b>admin</b>	<a href="#">Change username</a>
Password:	XXXXXXXXXX	<a href="#">Change password</a>

[Back to Prev page](#)

## Network statistics page

As a new feature of the Next series of products, you can monitor the live traffic flows over the link. These figures are showing the reception on a port of FO(fibre optic from the remote end) or TP(Twisted pair, form the local connected equipment).

Network statistics		
	FO Port	TP Port
Unicast:	0	674
Multicast:	0	558
Broadcast:	0	2098
Fragments:	0	0
Jabbers:	0	0
Alignment error:	0	0
Symbol error:	0	0
CRC error:	0	0
Elapsed time : [0000:15:13]		<input type="button" value="CLEAR"/>

[Back to Prev page](#)

Unicast: sending of information packets to a single destination

Multicast: is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once and only create copies when the links to the destinations split. The word "Multicast" is typically used to refer to IP Multicast, the implementation of the multicast concept on the IP routing level, where routers create optimal spanning tree distribution paths for datagram sent to a multicast destination address in real-time. But there are also other implementations of the multicast distribution strategy listed below.

Broadcast: refers to transmitting a packet that will be received (conceptionally) by every device on the network. In practice, the scope of the broadcast is limited to a broadcast domain. Not all computer networks support broadcasting; for example, neither X.25 nor frame relay supply a broadcast capability, nor is there any form of Internet-wide broadcast. Broadcasting is largely confined to local area network (LAN) technologies, most notably Ethernet and Token Ring, where the performance impact of broadcasting is not as large as it would be in a wide area network. Both Ethernet and IPv4 use an all-ones broadcast address to indicate a broadcast packet.

Fragments: datagram can be fragmented into pieces small enough to pass over a link with a smaller MTU than the original datagram size.

Jabber: transmission of a packet on a computer network that is larger than the network's MTU. Such transmissions hog bandwidth and congest the network. Many network switches have a built-in capability to detect when a device is jabbering and block it until it resumes proper operation.

Alignment error:Decoded package alignment is faulty.

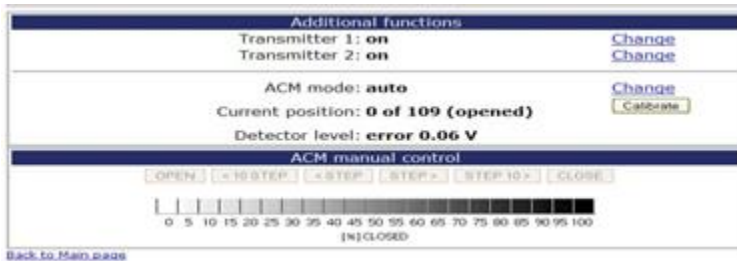
Symbol error: Coding symbol is missing or faulty.

CRC error: cyclic redundancy check is a type of hash function used to produce a checksum – a small, fixed number of bits – against a block of data, such as a packet

of network traffic or a block of a computer file. The checksum is used to detect errors after transmission or storage. A CRC is computed and appended before transmission or storage, and verified afterwards by the recipient to confirm that no changes occurred on transit. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channel.

## PX-P3000E100TP0 extra MGM features

Additional functions



Transmitter on and off: you can switch the transmitters on and off individually.

ACM: (aperture control mechanism)



Default: auto mode, the system will automatically regulate the incoming light to the optimal level of Udet, preventing the system to get oversaturated.

Manual: The incoming light can be regulated manually; the use of the manual mode is strongly suggested during installation. The controller won't start the regulation of the incoming light, so the alignment will be much more accurate. (it can be set by doing an unfinished booting during log in so we do not have to log on to the web during the installation process).

Calibrating: it is an extra service. Some silencing settings can be made manually (according to the scale) and the motor can also be skipped manually via the web. In order to see where the motor is there are cadences. The system has to make a calibration of the length of the circuit between the two end station in order to see how many steps are left. Follow-up calibration can be made with the calibrate button.



## Mandatory Management Activation

Thank you for buying our product. Please read this note carefully. From software version (3.2.1218/R090x)!

The product you have bought has fully functional management software, which has limitation only in time. The unit activation request should be sent to [activation@geodesy-fso.com](mailto:activation@geodesy-fso.com). And the activation code will be issued, later and sent to the email address give, or can be accessed from your local distributor.

**After 90 days if the system was not activated the data transmission will be degraded!**


### Activation process:

1. Login to the devices through a web browser using the IP:192.168.100.220,192.168.100.221
2. Default login name:admin and password:admin

3. Click on Evaluation period

**BitView Web**  
**Evaluation period (240 hours remaining)**

4. Click on Get a key



BitView Web : Evaluation version  
Please activate the system!  
Key:

5. Fill in the table and click on send



FSO HEAD 1: Evaluation window - Netscape Navigator  
http://192.168.100.221/evalform.htm  
FSO HEAD 1: Evaluation window  
BitView Web : Evaluation form  
Name:   
Company:   
Email:   
  
[Back to Main page](#)

6. We will return the activation key

### Limitations:

- All Next-Series(100MB/s) limitation course 1-60 days unlimited, for 61-80 days 10MB/s, for 81-90 days 1MB/s, beyond 90 days 100KB/s (MGM-Option).
- All GigaNext-Series(1000 MB/s) will be limited after the 90<sup>th</sup> day, when the whole bandwidth will be blocked, except the management system.

## 8.2 Firmware update

Device Information	
Device name: <b>FSO HEAD 1</b> Managed head: <b>Pico-X (1)</b>	<a href="#">Change</a>
Detector alert level: <b>0.50 V</b> Temperature alert level: <b>70 °C</b>	<a href="#">Change</a> <a href="#">Change</a>
Auto MDI/MDI-X: <b>enabled</b> NPASD: <b>disabled</b>	<a href="#">Change</a> <a href="#">Change</a>
Motherboard Serial number: <b>000001</b> Head Serial number: <b>0000001</b>	
Software version: <b>3.2.1204 / 084C</b> Uploaded software: <b>none</b>	<b>(factory)</b> <a href="#">Update</a>

[Back to Main page](#)

The firmware update has the following steps:

Run FTP client  
Log-in to the Laser-head  
Copy Geodesy\_FWUpdate\_Vxx.xbn over  
Log in the laserhead  
Click on update  
Wait 50-60 seconds  
Restart the laserhead

Run FTP client  
FTP client setup  
IP address: the IP address of the device (192.168.100.220 or 192.168.100.221 as a factory default ) or the IP address you gave to the system earlier – same as the IP address for the Web management.

User name: same as for the web management (default admin)

Password: same as for the web management (default admin)

If you have passive mode please turn it off, otherwise the system will not connect.

[-0-] ftp://192.168.100.221			
0:\*.*			
Név	Kit.	Méret	↓Dátum
[-.]			<DIR> 1980.00.01
core	sys	4 096	2008.04.01

copy the .xbn file over to the Laserhead

0:\*.*			
Név	Kit.	Méret	↓Dátum
[-.]			<DIR> 1980.00.01
update	xbn	?	2008.06.01
core	sys	4 096	2008.04.01

Log off the FTP server

Now the Update button will be active

Device Information	
Device name: <b>FSO HEAD 1</b> Managed head: <b>Pico-X (1)</b>	<a href="#">Change</a>
Detector alert level: <b>0.50 V</b> Temperature alert level: <b>70 °C</b>	<a href="#">Change</a> <a href="#">Change</a>
Auto MDI/MDI-X: <b>enabled</b> NPASD: <b>disabled</b>	<a href="#">Change</a> <a href="#">Change</a>
Motherboard Serial number: <b>228855</b> Head Serial number: <b>0000001</b>	
Software version: <b>3.2.1204 / 084C</b> Uploaded software: <b>3.2.1206 / 086C (U)</b>	<b>(factory)</b> <input type="button" value="Update"/>

[Back to Main page](#)

Click on update and the update process will start it takes upto 60 seconds. The LEDs on the back of the device will go off than lit one after the other.

Make sure that the system power is fixed and the power will not go off during the update process. If the LEDs froze, wait 2-3 minutes before unplugging the power cable, and replugging again.

## 8.3 Reloading factory default settings

Should you need to reload the original factory settings follow the steps below.

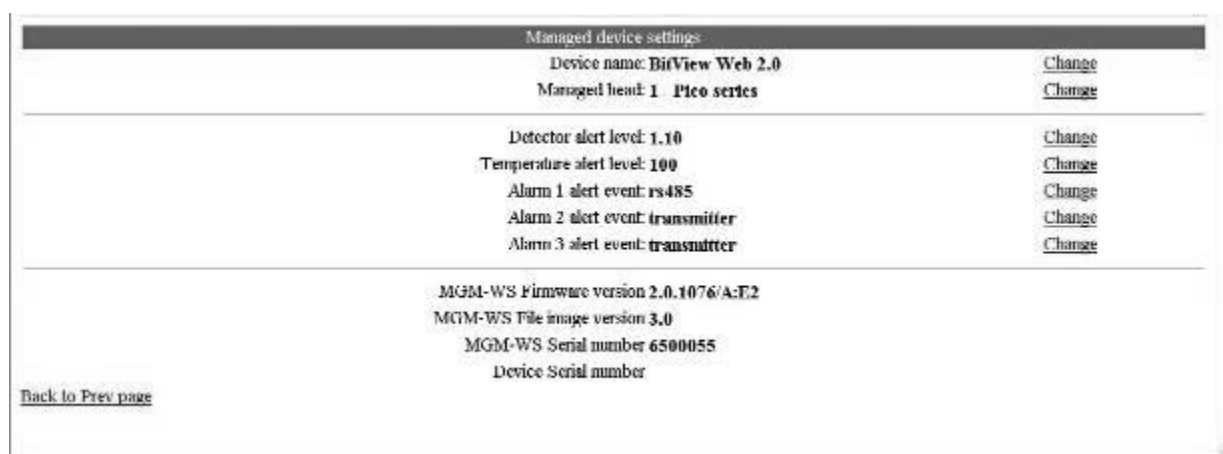
1. unplug the POE RJ45 cable
2. replug the POE RJ45 cable
3. unplug the POE RJ45 cable within 3 seconds
4. repeat procedure 3 times.
5. plug the POE RJ45 cable into the system, and leave it plugged in.

After this the system resets the following information to the factory default.

- IP address
- Username
- Password
- Device name
- SNMP settings
- Alerts
- Auto MDI/MDIX
- NPASD (if available): if the receiver does not detect sufficient light power, then in the head would switch off the network connection signal. Note: During this period the 100MB/s laser heads MGM will not be available.

## 8.4 Setting up the SNMP

Please check the GD view manual for details how to proceed to this point



1. Figure

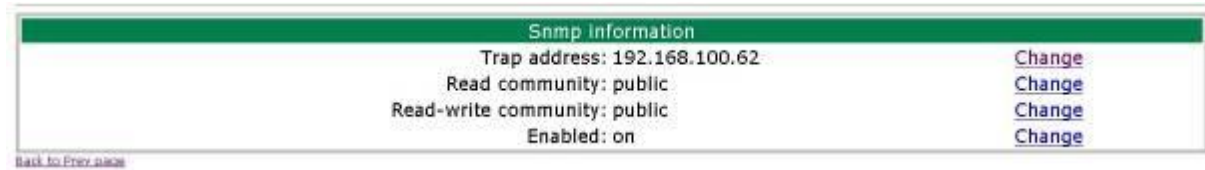
On Figure 1 you can see our test setting. The GD-View is sending 3 traps  
**LaserHeadAlarm** (OID: 1.3.6.1.4.1.17857.0.1201) This trap will be sent after any of the alarms will go on (for alarm setting please see chapter 5.4)

**LaserHeadAlarmCancel** (OID: 1.3.6.1.4.1.17857.0.1202) After the alarm goes off this trap will be sent

**DeviceDown** (OID: 1.3.6.1.4.1.17857.0.1103) This trap is being sent when the SNMP agent is disabled

Even if you have one laerhead attached to one GD-View, or you are on the live network you can generate traps without, causing any problems, with the testing.

For these testing purposes please set Alarm1 to RS485(this will generate traps), and Alarm2 Alarm3 to transmitter(this wont generate traps, so wont disturb the testing)



**2. Figure**

On figure 2 the settings can be seen.

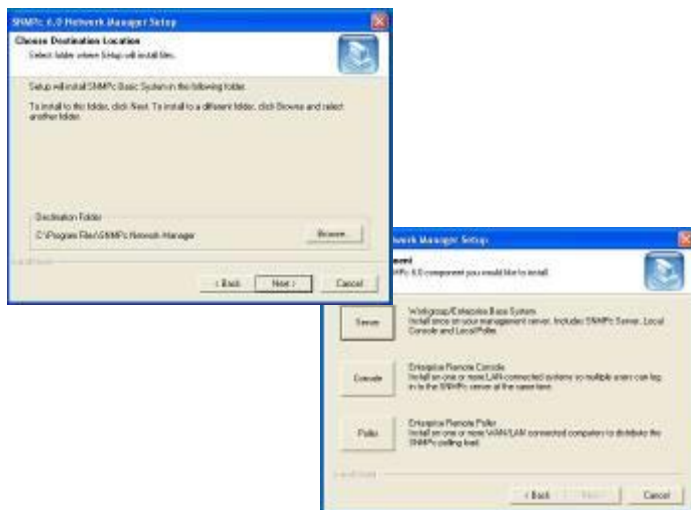
Change the Trap address to the MGM console IP address which will have the SMNPc installed

Enabled must be set to on the function will disable the SNMP agent.

After this was set the GD view is ready to send out the Trap messages, to the Trap Addressed PC

### 8.4.1 SNMPc Installation

First run snmpc600eval.exe file from the CD.



Run through the setup process by clicking next

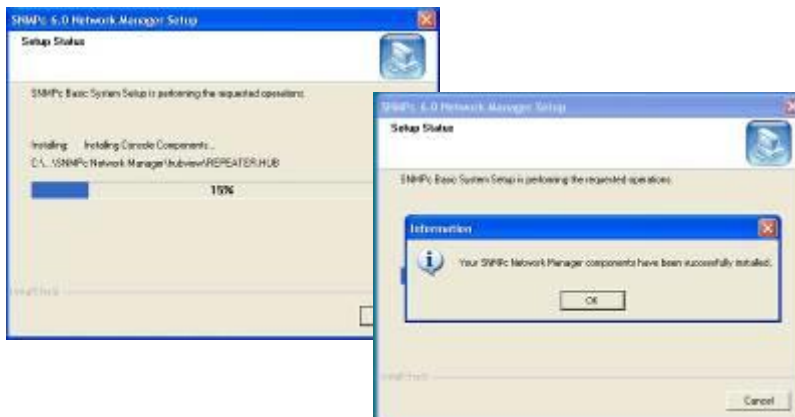


When the setup asks for the discovery seed enter you own IP address, Subnet mask a community

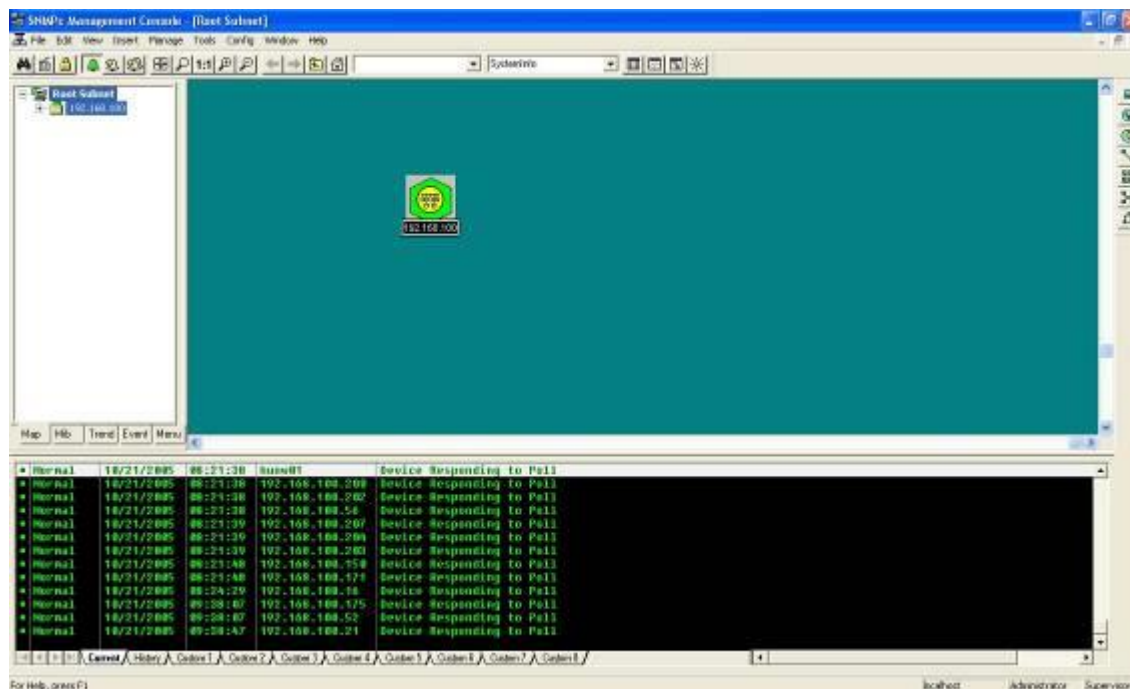
After the setup was finished hit OK. Your PC might ask for a restart, in that cases please restart your PC

## SNMPC

### 8.4.2 Configuration of the SNMPC Management console

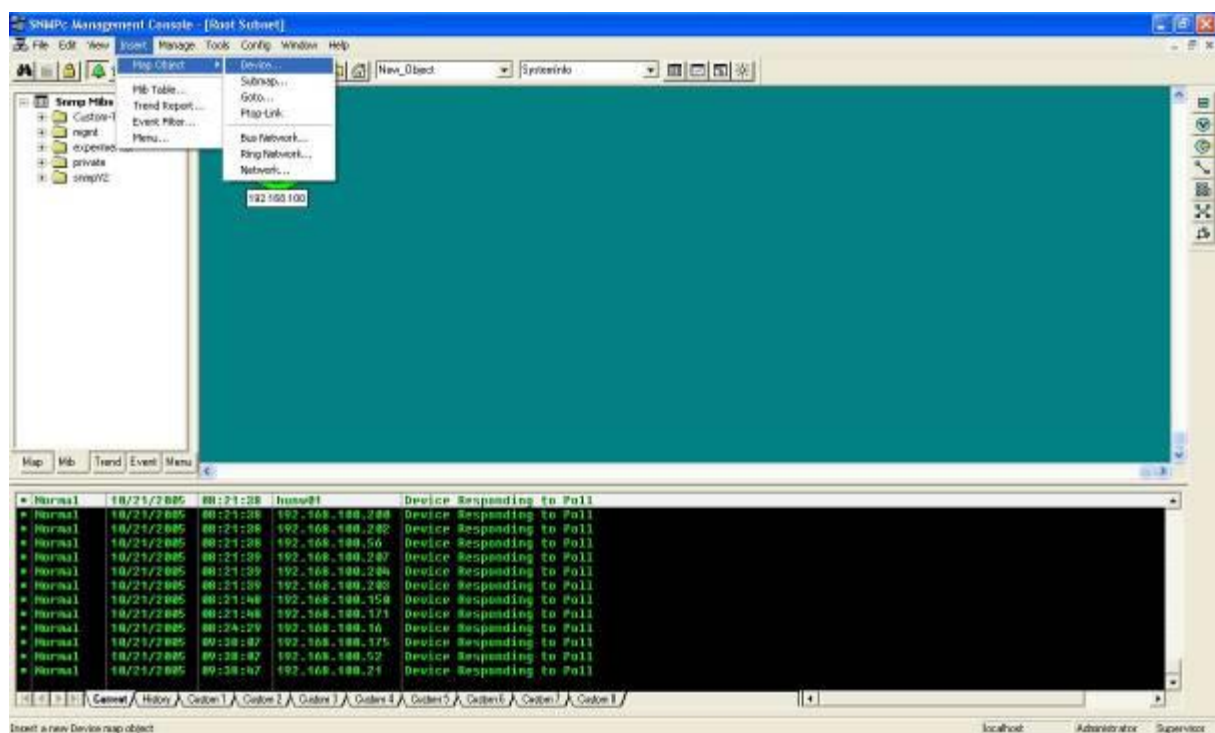


Click on Start => Programs => SNMPc network manager => Startup system. This will start the SNMPc Management console. Can be seen on Figure 3



3. Figure

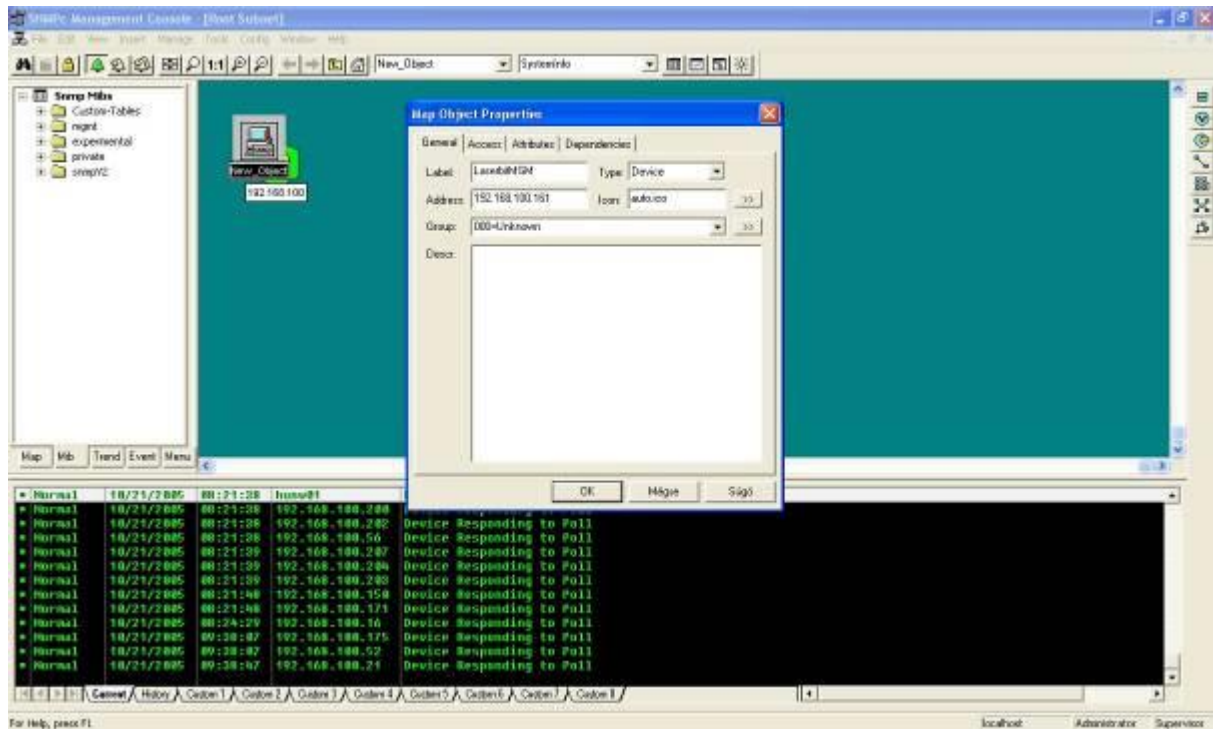
To add the GD-View to the console click on Insert => Map Object => Device. As it is shown on Figure 4



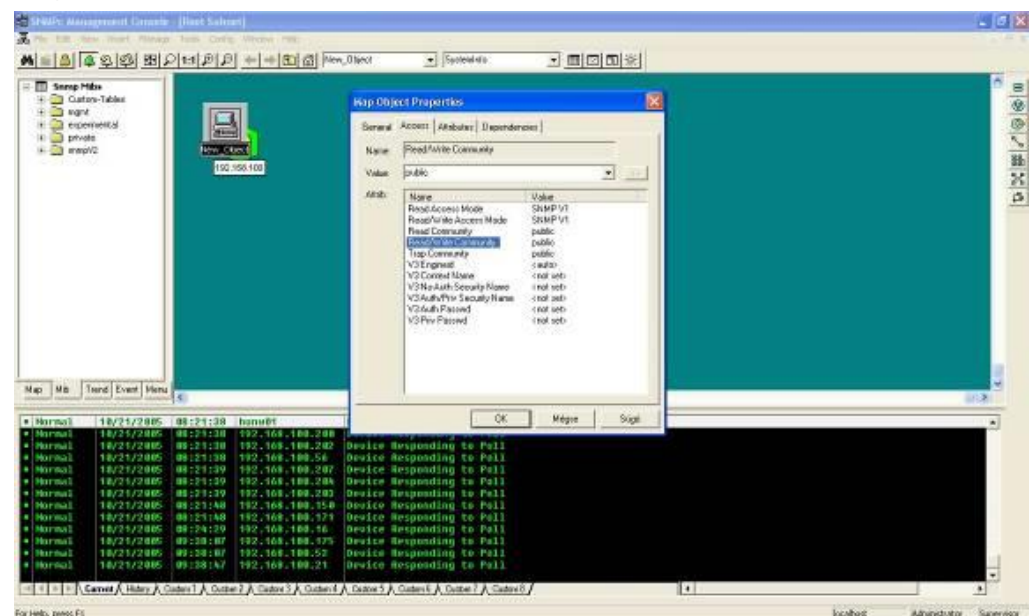
4. Figure



After the Map Object was added, the properties should be set:  
Label : GeoDesy-FSO MGM (cannot contain spaces, or special caracters) see Figure



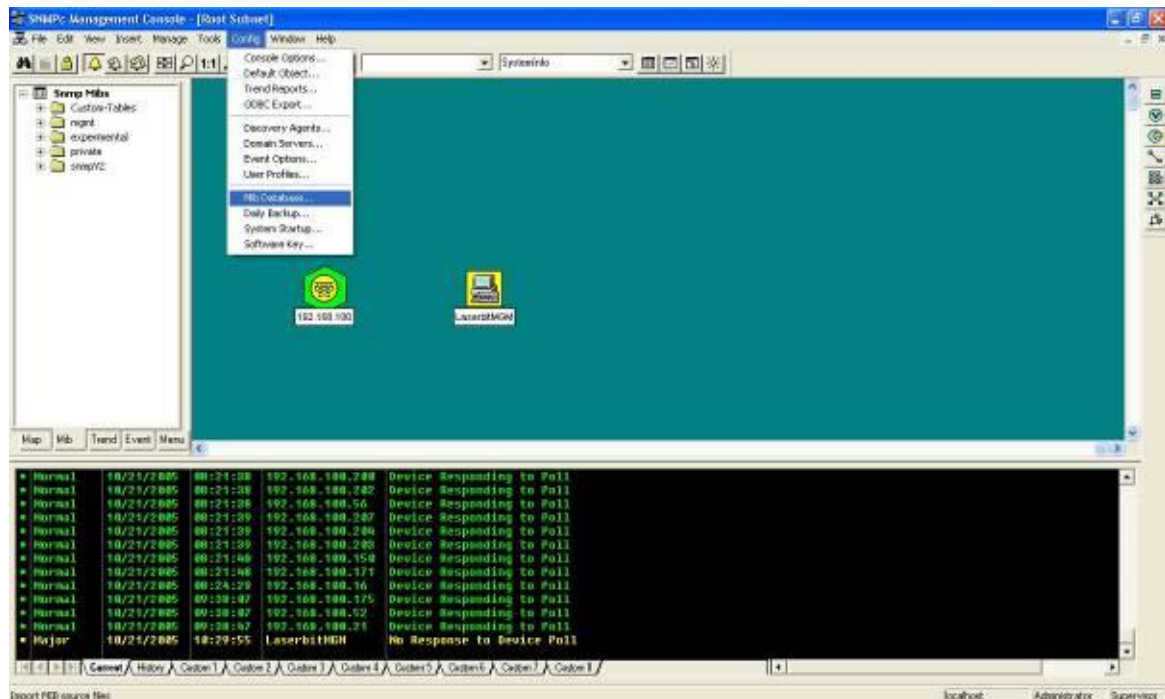
On the Access Tab  
Read Access Mode: SNMPV1  
Read/Write Access Mode: SNMPV1  
Read community: public  
Read/Write Community: public  
Trap community: public  
The rest of the setting can be left on factory default.



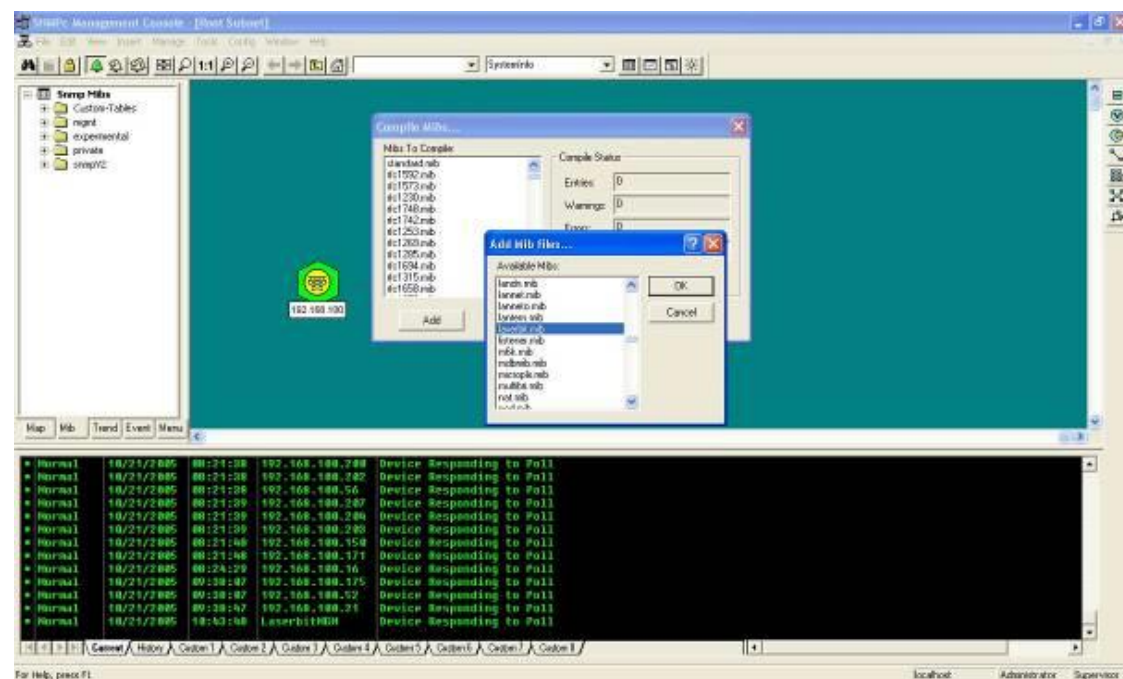
### 8.4.3 Compiling GeoDesy-FSO Mib file

First copy the Mib file (GeoDesy-FSO.mib [Source: CD:\Mib\V07\GeoDesy-FSO.mib]). Copy this file over to : C:\Program Files\SNMPC Network Manager\mibfiles\

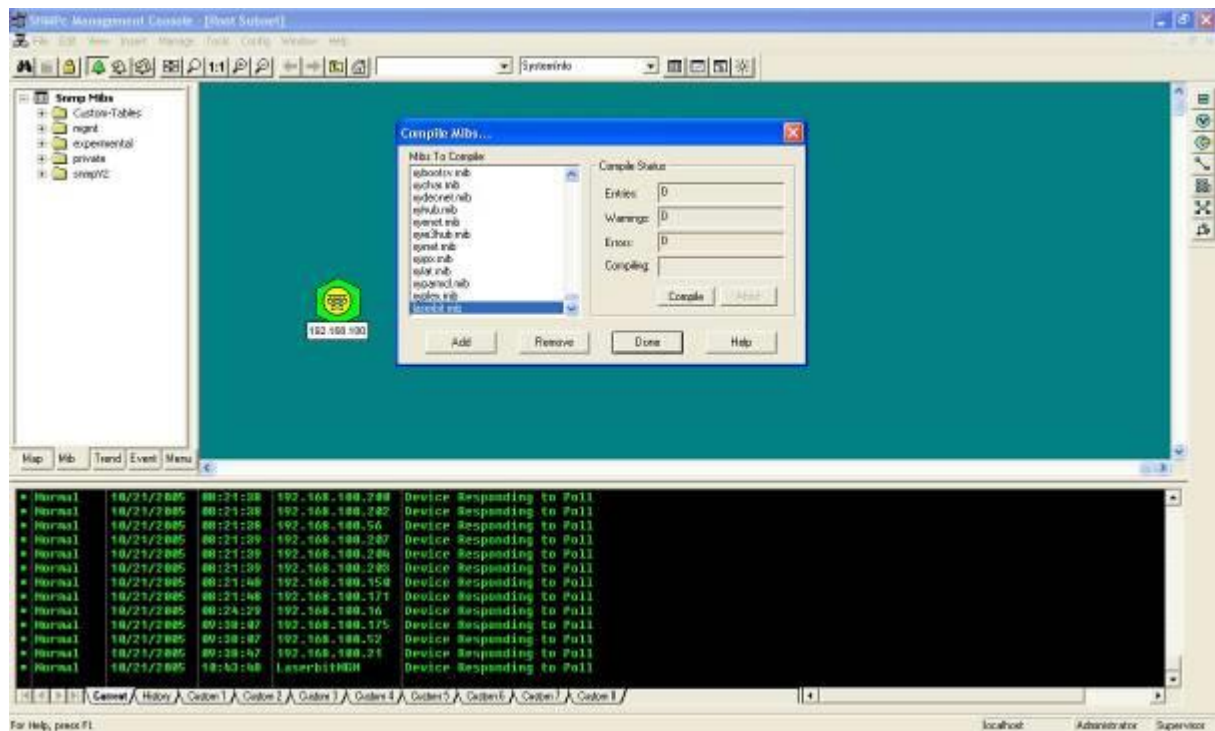
To Compile the MIB file to the SNMPc Click on Config=>Mib Database



After opening the Mib Database, you should add the MIB file to the Database: Click on Add. Add Mib files: find GeoDesy-FSO.mib, then click OK



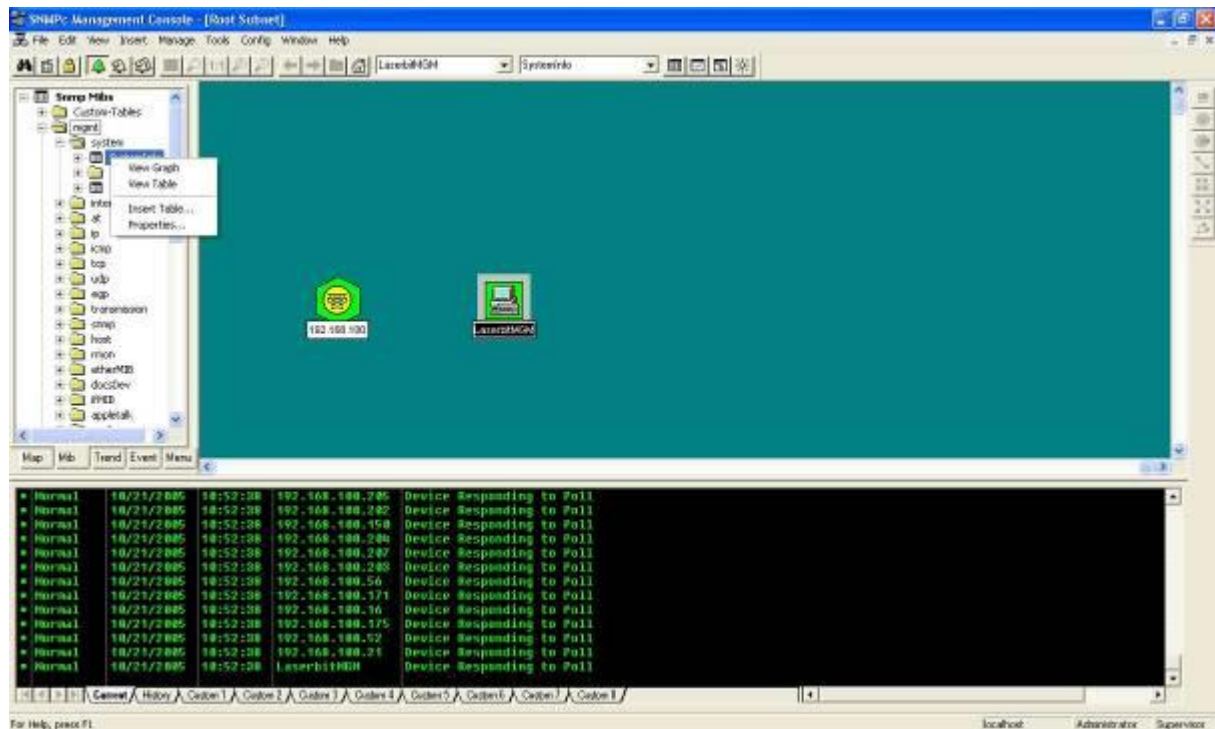
After you hit OK you have added the Mib file to the database now you will have to compile it to the management console. So find again GeoDesy-FSO.mib and highlight it. Than Hit compile. It will ask you whether you want to compile it click on Yes.



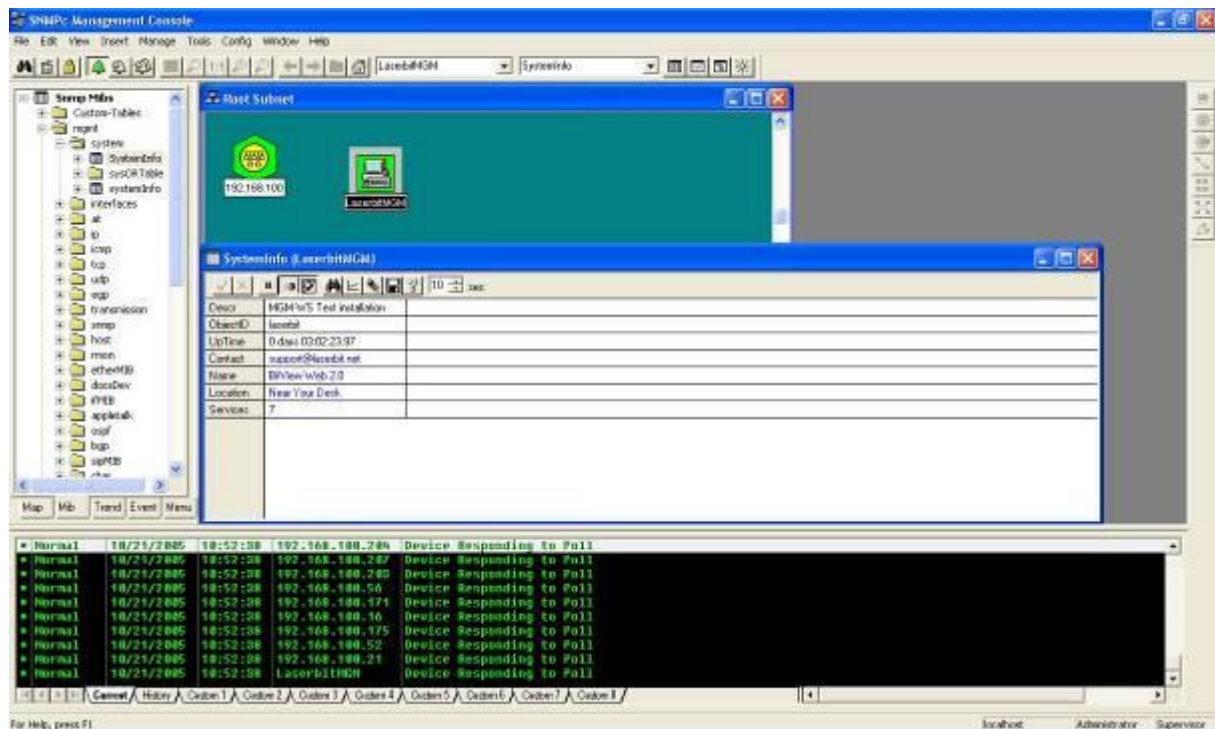
## 8.4.4 Using SNMP to monitor the link

First click on the GeoDesy-FSO Object to highlight it.

Open mgmt/system/SystemInfo right click on the object and view Table

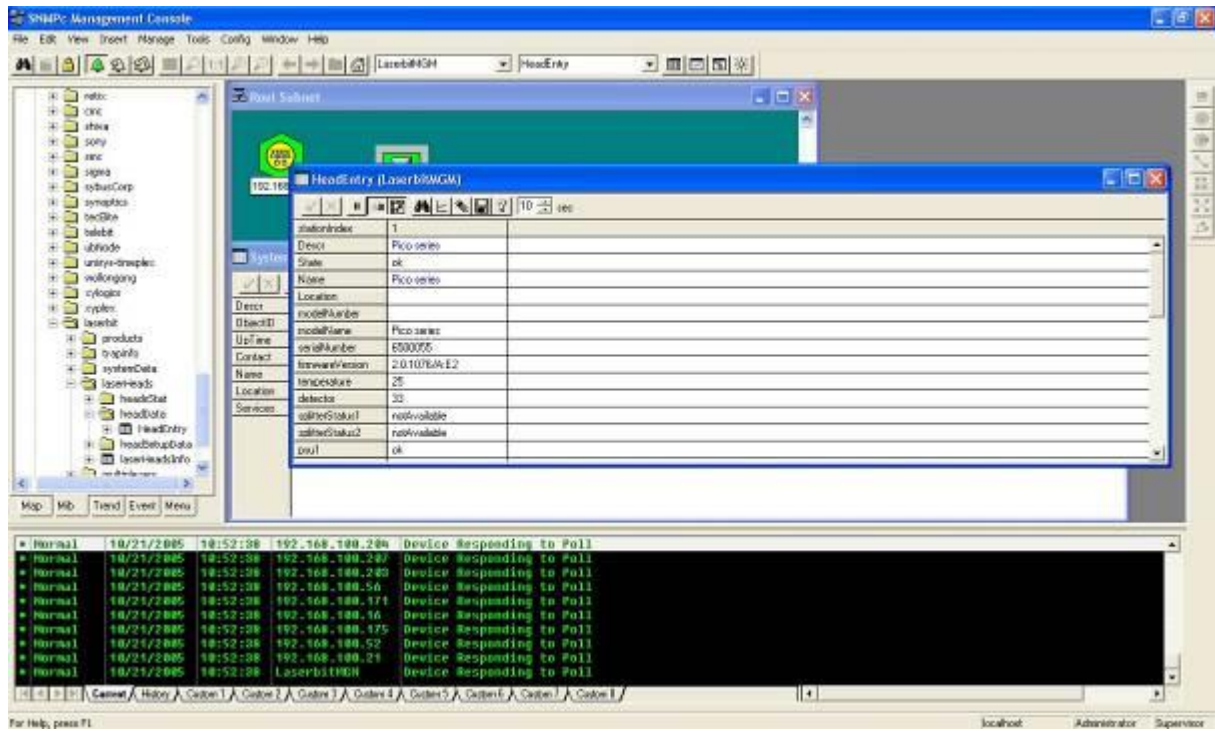


This table will show you the main System information Table:



To see the head entries open: private/GeoDesy-FSO/headData  
Right click on the head entry table and view table.





Now the SNMP is completely set up.

While the SNMP is working, if you would like to see that actually, it really does what it suppose to be, unplug the RJ11 (RS485) cable from the GD-View.

[illegible]

After reconnecting the RS485 cable the trap message should arrive that the alarm was canceled  
You can acknowledge the alarm with a right click on the alarm.

The screenshot displays the SHAPC Management Console interface. The top menu bar includes File, Edit, View, Insert, Manage, Tools, Config, Window, and Help. The left sidebar shows a tree view of the system structure, including folders like 'netio', 'chic', 'shiva', 'sony', 'nuc', 'sigrid', 'systemCorp', 'systemData', 'systemInfo', 'systemLog', 'systemMap', 'systemTime', 'systemUser', 'systemWeb', 'systemWeb2', 'systemWeb3', 'systemWeb4', 'systemWeb5', 'systemWeb6', 'systemWeb7', 'systemWeb8', 'systemWeb9', 'systemWeb10', 'systemWeb11', 'systemWeb12', 'systemWeb13', 'systemWeb14', 'systemWeb15', 'systemWeb16', 'systemWeb17', 'systemWeb18', 'systemWeb19', 'systemWeb20', 'systemWeb21', 'systemWeb22', 'systemWeb23', 'systemWeb24', 'systemWeb25', 'systemWeb26', 'systemWeb27', 'systemWeb28', 'systemWeb29', 'systemWeb30', 'systemWeb31', 'systemWeb32', 'systemWeb33', 'systemWeb34', 'systemWeb35', 'systemWeb36', 'systemWeb37', 'systemWeb38', 'systemWeb39', 'systemWeb40', 'systemWeb41', 'systemWeb42', 'systemWeb43', 'systemWeb44', 'systemWeb45', 'systemWeb46', 'systemWeb47', 'systemWeb48', 'systemWeb49', 'systemWeb50', 'systemWeb51', 'systemWeb52', 'systemWeb53', 'systemWeb54', 'systemWeb55', 'systemWeb56', 'systemWeb57', 'systemWeb58', 'systemWeb59', 'systemWeb60', 'systemWeb61', 'systemWeb62', 'systemWeb63', 'systemWeb64', 'systemWeb65', 'systemWeb66', 'systemWeb67', 'systemWeb68', 'systemWeb69', 'systemWeb70', 'systemWeb71', 'systemWeb72', 'systemWeb73', 'systemWeb74', 'systemWeb75', 'systemWeb76', 'systemWeb77', 'systemWeb78', 'systemWeb79', 'systemWeb80', 'systemWeb81', 'systemWeb82', 'systemWeb83', 'systemWeb84', 'systemWeb85', 'systemWeb86', 'systemWeb87', 'systemWeb88', 'systemWeb89', 'systemWeb90', 'systemWeb91', 'systemWeb92', 'systemWeb93', 'systemWeb94', 'systemWeb95', 'systemWeb96', 'systemWeb97', 'systemWeb98', 'systemWeb99', 'systemWeb100'. The main window is divided into three panes. The top pane shows a 'SystemInfo (LaserbitMGM)' table with columns for 'Device', 'ObjectID', 'Uptime', 'Contact', 'Name', 'Location', and 'Services'. The middle pane shows a 'HeadEntry (LaserbitMGM)' table with columns for 'Device', 'ObjectID', 'Uptime', 'Contact', 'Name', 'Location', and 'Services'. The bottom pane shows a log of events, including 'Normal' and 'Error' messages, with a context menu open over the log entries. The context menu options are: Properties..., Locate Object, Add Entry, Copy, Cut, Paste, Delete, and Del. The log entries show 'Device Responding to Poll' messages for various devices, including 'LaserbitMGM' and 'LaserbitMGM-101'. The status bar at the bottom indicates 'For Help, press F1' and 'localhost Administrator Supervisor'.

Device	ObjectID	Uptime	Contact	Name	Location	Services
MGM/WS Test installation	laserbit	0 days 03:10:15:25	support@laserbit.net	EFView/WEB 2.0	New York Desk	7

Device	ObjectID	Uptime	Contact	Name	Location	Services
laserbit	laserbit	0 days 03:10:15:25	support@laserbit.net	EFView/WEB 2.0	New York Desk	7

Log entries:

- Normal 10/21/2005 10:52:30 192.168.100.280 Device Responding to Poll
- Normal 10/21/2005 10:52:30 192.168.100.56 Device Responding to Poll
- Normal 10/21/2005 10:52:30 192.168.100.171 Device Responding to Poll
- Normal 10/21/2005 10:52:30 192.168.100.16 Device Responding to Poll
- Normal 10/21/2005 10:52:30 192.168.100.175 Device Responding to Poll
- Normal 10/21/2005 10:52:30 192.168.100.52 Device Responding to Poll
- Normal 10/21/2005 10:52:30 192.168.100.71 Device Responding to Poll
- Normal 10/21/2005 10:52:30 LaserbitMGM Device Responding to Poll
- Normal 10/21/2005 11:00:09 LaserbitMGM Laserbit-Traps.101 [1] laserHeadRlarm.0 (Integer): 0 [2] shmptrapEnterprise.0 (Object ID): laserbit
- Error 10/21/2005 11:01:00 LaserbitMGM Laserbit-Traps.101 [1] laserHeadRlarmCancel.0 (Integer): 0 [2] shmptrapEnterprise.0 (Object ID): laserbit



## 8.4.6 SNMP Technology

SNMP is part of the Internet network management architecture. This architecture is based on the interaction of many entities, as described in the following section.

### The Internet Management Model

As specified in Internet RFCs and other documents, a network management system comprises:

*Network elements* -- Sometimes called *managed devices*, network elements are hardware devices such as computers, routers, and terminal servers that are connected to networks.

*Agents* -- Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.

*Managed object* -- A managed object is a characteristic of something that can be managed. For example, a list of currently active TCP circuits in a particular host computer is a managed object. Managed objects differ from variables, which are particular object instances. Using our example, an object instance is a single active TCP circuit in a particular host computer. Managed objects can be scalar (defining a single object instance) or tabular (defining multiple, related instances).

*Management information base (MIB)* -- A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.

*Syntax notation* -- A syntax notation is a language used to describe a MIB's managed objects in a machine-independent format. Consistent use of a syntax notation allows different types of computers to share information. Internet management systems use a subset of the International Organization for Standardization's (ISO's) *Open System Interconnection (OSI) Abstract Syntax Notation 1 (ASN.1)* to define both the packets exchanged by the management protocol and the objects that are to be managed.

*Structure of Management Information (SMI)* -- The SMI defines the rules for describing management information. The SMI is defined using ASN.1.

*Network management stations (NMSs)* -- Sometimes called *consoles*, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.

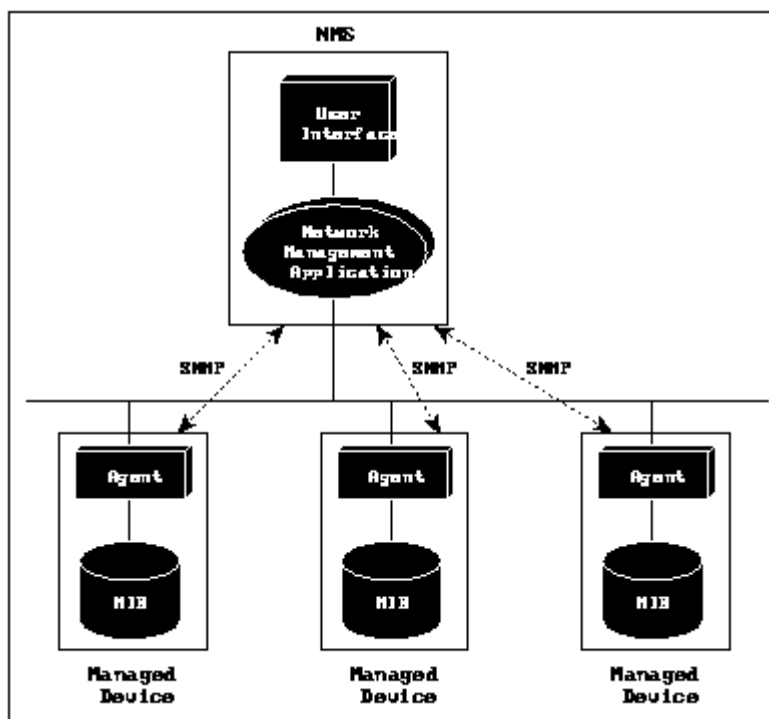
*Parties* -- Newly defined in SNMPv2, a party is a logical SNMPv2 entity that can initiate or receive SNMPv2 communication. Each SNMPv2 party comprises a single, unique party identity, a logical network location, a single authentication protocol, and a single privacy protocol. SNMPv2 messages are communicated between two

parties. An SNMPv2 entity can define multiple parties, each with different parameters. For example, different parties can use different authentication and/or privacy protocols.

*Management protocol* -- A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

The most basic elements of the Internet management model are graphically represented in *Figure 1*.

**Figure 1: The Internet Management Model**



Interactions between the NMS and managed devices can be any of four different types of commands:

*Reads* -- To monitor managed devices, NMSs read variables maintained by the devices

*Writes* -- To control managed devices, NMSs write variables stored within the managed devices

*Traversal operations* -- NMSs use these operations to determine which variables a managed device supports and to sequentially gather information from variable tables (such as IP routing tables) in managed devices

*Traps* -- Managed devices use traps to asynchronously report certain events to NMSs

## **MIBs and Object Identifiers**

A MIB can be depicted as an abstract tree with an unnamed root. Individual data items make up the leaves of the tree. *Object identifiers* (IDs) uniquely identify or name MIB objects in the tree. Object IDs are like telephone numbers -- they are organized hierarchically with specific digits assigned by different organizations.

The object ID structure of an SNMP MIB defines three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT. Much of the current MIB activity occurs in the portion of the ISO branch defined by object identifier 1.3.6.1 and dedicated to the Internet community.

The current Internet-standard MIB, MIB-II, is defined in RFC 1213 and contains 171 objects. These objects are grouped by protocol (including TCP, IP, *User Datagram Protocol* [UDP], SNMP, and others) and other categories, including "system" and "interfaces."

## SMI Definitions

The SMI specifies that all managed objects should have a name, a syntax, and an encoding. The *name* is the object ID, which was discussed in the preceding section. The *syntax* defines the object's data type (for example, "integer" or "string"). A subset of ASN.1 definitions are used for the SMI syntax. The *encoding* describes how the information associated with the managed object is formatted as a series of data items for transmission on the network. Another ISO specification, called the *Basic Encoding Rules* (BERs), details SMI encodings.

SMI data types are divided into three categories: *simple types*, *application-wide types*, and *simply constructed types*.

Simple types include four primitive ASN.1 types:

*Integers* -- Unique values that are positive or negative whole numbers, including zero.

*Octet strings* -- Unique values that are an ordered sequence of zero or more octets.

*Object IDs* -- Unique values from the set of all object identifiers allocated according to the rules specified in ASN.1.

*Bit strings* -- New in SNMPv2, these comprise zero or more named bits that specify a value.

Application-wide data types refer to special data types defined by the SMI:

*Network addresses* -- Represent an address from a particular protocol family.

*Counters* -- Non-negative integers that increment by positive one until they reach a maximum value, when they are reset to zero. The total number of bytes received on an interface is an example of a counter. In SNMPv1, counter size was not specified. In SNMPv2, 32-bit and 64-bit counters are defined.

*Gauges* -- Non-negative integers that can increase or decrease, but latch at a maximum value. The length of an output packet queue (in packets) is an example of a gauge.

*Time ticks* -- Hundredths of a second since an event. The time since an interface entered its current state is an example of a tick.

*Opaque* -- Represents an arbitrary encoding. This data type is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.

*Integer* -- Represents signed, integer-valued information. This data type redefines the ASN.1 "integer" simple data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

*Unsigned integer* -- Represents unsigned integer-valued information. It is useful when values are always non-negative. This data type redefines the ASN.1 "integer" simple data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

Simply constructed types include two ASN.1 types that define multiple objects in tables and lists:

*Row* -- References a row in a table. Each element of the row can be a simple type or an application-wide type.

*Table* -- References a table of zero or more rows. Each row has the same number of columns.

ISO document 8825 (*Specification of Basic Encoding Rules for ASN.1*) defines ISO's BERs. The BERs allow dissimilar machines to exchange management information by specifying both the position of each bit within the transmitted octets and the structure of the bits. Bit structure is conveyed by describing the data type, length, and value.

The SMI for SNMPv2 includes two documents: RFCs 1443 and 1444. RFC 1443 (Textual Conventions) defines the data types used within the MIB modules, while RFC 1444 (Conformance Statements) provides an implementation baseline. The SNMPv2 SMI also defines two new branches of the Internet MIB tree: security (1.3.6.1.5) and SNMPv2 (1.3.6.1.6).

## **SNMP Operations**

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response. Six SNMP operations are defined:

*Get* -- Allows the NMS to retrieve an object instance from the agent.

*GetNext* -- Allows the NMS to retrieve the next object instance from a table or list within an agent. In SNMPv1, when an NMS wants to retrieve all elements of a table from an agent, it initiates a *Get* operation, followed by a series of *GetNext* operations.

*GetBulk* -- New for SNMPv2. The GetBulk operation was added to make it easier to acquire large amounts of related information without initiating repeated get-next operations. GetBulk was designed to virtually eliminate the need for GetNext operations.

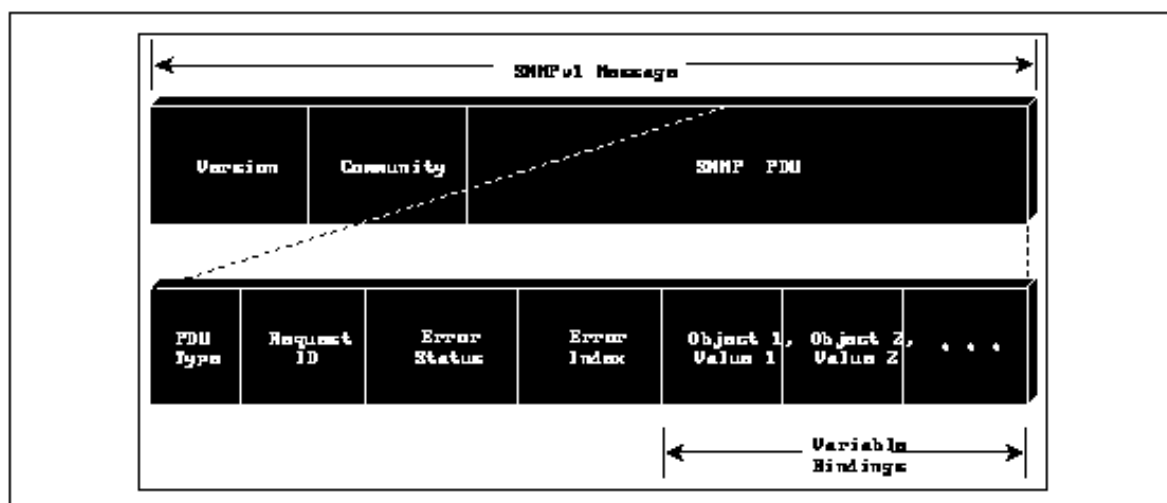
*Set* -- Allows the NMS to set values for object instances within an agent.

*Trap* -- Used by the agent to asynchronously Inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

*Inform* -- New for SNMPv2. The Inform operation was added to allow one NMS to send trap information to another.

SNMPv1 messages (packets) contain two parts<sup>1</sup>. The first part contains a *version* and a *community name*. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed ("Get," "Set," and so on) and the object instances involved in the operation. Figure 3 illustrates the SNMPv1 message format.

**Figure 3: SNMP v1 Message Format**



\* Trap messages have a slightly different format; for information on this format, consult the appropriate SNMP specification.

The version field is used to ensure that all network elements are running software based on the same SNMP version. The community name assigns an access environment for a set of NMSs using that community name. NMSs within the community can be said to exist within the same administrative domain. Because devices that do not know the proper community name are precluded from SNMP operations, network management personnel also have used the community name as a weak form of authentication.

The SNMP PDU has the following fields:

*PDU type* -- Specifies the type of PDU being transmitted.

*Request-ID* -- Associates requests with responses.

*Error-status* -- Indicates an error and an error type. In SNMPv2 GetBulk operations, this field becomes a NonRepeaters field. For these operations, this field defines the

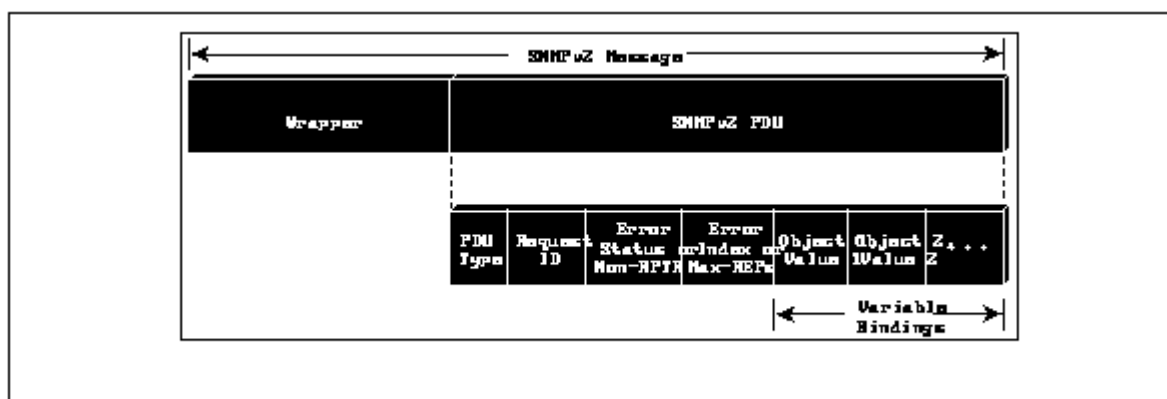
number of request-ed variables listed that should be retrieved no more than once from the beginning of the request. The field is used when some of the variables are scalar objects with only one variable.

*Error-index* -- Associates the error with a particular object instance. In SNMPv2 GetBulk operations, this field becomes a Max Repetitions field. For these operations, this field defines the maximum number of times that other variables beyond those specified by the NonRepeaters field should be retrieved.

*Variable-bindings* -- Comprises the data of an SNMP PDU. Variable bindings associate particular object instances with their current values.

Like SNMPv1 messages, SNMPv2 messages (shown in *Figure 4*) contain two parts. The second part of the SNMPv2 message (the PDU) is virtually identical to that of an SNMPv1 message (see the previous description of an SNMP PDU for differences). The first part of the SNMPv2 message contains the majority of the differences between SNMPv1 and SNMPv2.

**Figure 4: SNMP v2 Message Format**



The first part of a SNMPv2 message is often called a *wrapper*. The wrapper includes authentication and privacy information in the form of destination and source parties. As mentioned earlier, a party includes the specification of both an authentication and a privacy protocol. In addition to a destination and a source party, the wrapper includes a *context*. A context specifies the managed objects visible to an operation. The authentication protocol is designed to reliably identify the integrity of the originating SNMPv2 party. It consists of authentication information required to support the authentication protocol used. The privacy protocol is designed to protect information within the SNMPv2 message from disclosure. Only authenticated messages can be protected from disclosure. In other words, authentication is required for privacy.

The SNMPv2 specifications discuss two primary security protocols: one for authentication and one for privacy. These are the *Digest Authentication Protocol* and the *Symmetric Privacy Protocol*.

The Digest Authentication Protocol verifies that the message received is the same one that was sent. Data integrity is protected using a 128-bit *message digest* calculated according to the Message Digest 5 (MD5) algorithm. The digest is calculated at the sender and enclosed with the SNMPv2 message. The receiver

verifies the digest. A secret value, known only to the sender and the receiver, is prefixed to the message. After the digest is used to verify message integrity, the secret value is used to verify the message's origin.

To help ensure message privacy, the Symmetric Privacy Protocol uses a secret encryption key known only to the sender and the receiver. Before the message is authenticated, this protocol uses the *Data Encryption Standard* (DES) algorithm to effect privacy. DES is a documented *National Institute of Standards and Technology* (NIST) and *American National Standards Institute* (ANSI) standard.

Originally, SNMPv1 specified that SNMP should operate over the *User Datagram Protocol* (UDP) and IP. The SNMPv2 transport mapping document (RFC 1449) defines implementations of SNMP over other transport protocols, including *OS/Connectionless Network Service* (CLNS), AppleTalk's *Datagram Delivery Protocol* (DDP), and Novell's *Internet Packet Exchange* (IPX). RFC 1449 also includes instructions on how to provide a SNMPv1 proxy and use of the BER. UDP/IP is still SNMPv2's preferred transport mapping because UDP is compatible with SNMPv1 at both the transport and network layers.



## Trap event list

Alert disabled: there is no alert coming up for this trap

Temperature: The agent will send an alarm if the value goes above the preset value.

For further details please see *Temperature alert level in the **Device Setup*** chapter.

Detector: The agent will send an alarm if the value goes above the preset value. For

further details please see *Detector alert level in the **Device Setup*** chapter.

Transmitter: if the transmitter fails operating the agent will send an alarm.

Power supply: if the power supply reports fault the agent will send the alarm.

Receiver: If the receiver gets into disabled the agent will send an alarm. For further details please see *RX OK* in the **Status info screen** chapter

Remote Failure: If the local head loses the connection to the remote head the agent will send an alarm. For further details please see *Remote is visible* in the **Status info screen** chapter

FSO Link: The Agent will send an alarm if the valid signal is lost. . For further details please see *FSO Link* in the **Status info screen** chapter.

TP Link: The Agent will send an alarm if the connection is lost on the local TP port.

For further details please see *TP\_Link* in the **Status info screen** chapter.

Traffic error: The agent will send an alarm if any of the values on the *Network statistics page* is incremented.

## 9 Warranty conditions

**GeoDesy FSO (Europe) LTD** warrants that the **GeoDesy FSO** product purchased will be free from defects in material and workmanship for a period of one (1) year from the date of purchase. This warranty period will not be extended by virtue of a repair of the product or a replacement of any component of the product during the warranty period.

This warranty covers only normal commercial use. **GeoDesy FSO (Europe) LTD** is not responsible for warranty service should the **GeoDesy FSO** identification marks, serial numbers or original seals be removed, altered, or broken, or should the product fail to be properly maintained or fail to function properly as a result of any modification, misuse, abuse, improper installation, neglect, improper shipping, damage caused by disasters such as fire, flood, earthquake or lightning, improper electrical current, or service other than by **GeoDesy FSO (Europe) LTD** or its authorised partners.

If the **GeoDesy FSO** product fails to operate as warranted at any time during the warranty period, **GeoDesy FSO (Europe) LTD** will repair, or at its option, replace the defective product at no additional charge.

In no event will **GeoDesy FSO (Europe) LTD** be liable for any damages including loss of data, lost profits, lost savings, lost business, or other incidental or consequential or indirect damages arising out of the installation, use, maintenance, performance, failure or interruption of the **GeoDesy FSO** product, even if **GeoDesy FSO (Europe) LTD** has been advised of the possibility of such damage.

If you purchased the **GeoDesy FSO** product in the United States, some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation may not apply to you.

The purchaser or user shall have the responsibility to give **GeoDesy FSO (Europe) LTD** prompt written notice of any warranty claims. If the product was purchased through an authorised partner of **GeoDesy FSO (Europe) LTD**, notice may be given in writing to that authorised partner in the area in which the product was being used.

The product may be returned to **GeoDesy FSO (Europe) LTD** only if it has a Return Material Authorisation (RMA) number. The product must be shipped prepaid, insured and in the original shipping package or similar package for safe shipment. The RMA number must be marked on the outside of the shipping package. Any product returned without an RMA number shall be rejected.

Transportation charges for the return of the product will be paid by **GeoDesy FSO (Europe) LTD** if it is determined by **GeoDesy FSO (Europe) LTD** that the

product was defective within the terms of the warranty; otherwise the purchaser or user shall be responsible for costs of return handling and transportation.

If the **GeoDesy FSO** product does not operate as warranted above, the customer's sole remedy shall be repair or replacement. The foregoing warranties and remedies are exclusive and are in lieu of all other warranties, expressed or implied, either in fact or by operation of law, statutory or otherwise, including warranties of merchantability and fitness for a particular purpose. **GeoDesy FSO** neither assumes nor authorises any other person to assume for it any other liability in connection with the sale, installation, use or maintenance of the product.

## 10 Privacy statement

We will never share, sell, or rent individual personal information with anyone without your advance permission or unless ordered by a court of law. Information submitted to us is only available to employees managing this information for purposes of contacting you or sending you emails based on your request for information and to contracted service providers for purposes of providing services relating to our communications with you.